

1 Chief Judge Ricardo S. Martinez
2
3
4
5
6
7
8

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

10 UNITED STATES OF AMERICA,

11 Plaintiff,

12 v.

13 HUAWEI DEVICE CO., LTD., and
14 HUAWEI DEVICE USA, INC.,

15 Defendants.

16 NO. CR19-0010RSM

17
18 **GOVERNMENT'S RESPONSE TO
MOTION TO DISMISS FOR
SELECTIVE PROSECUTION, OR IN
THE ALTERNATIVE, FOR
DISCOVERY**

19
20 **(Noted August 30, 2019)**

21
22 The United States of America, by and through, Tessa M. Gorman, First Assistant
23 United States Attorney for the Western District of Washington (Acting Under Authority
24 Conferred by 28 U.S.C. § 515), and Todd Greenberg, Thomas Woods, and Siddharth
25 Velamoor, Assistant United States Attorneys for said District, hereby responds to
26 Defendants Huawei Device Co., Ltd. (“Huawei China”) and Huawei Device USA, Inc.
27 (“Huawei USA”) (collectively “Huawei”)’s motion to dismiss for selective prosecution,
28 or in the alternative, for discovery. Dkt. No. 57.

29
30 //
31 //
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
559
560
561
562
563
564
565
566
567
568
569
569
570
571
572
573
574
575
576
577
578
579
579
580
581
582
583
584
585
586
587
588
589
589
590
591
592
593
594
595
596
597
598
599
599
600
601
602
603
604
605
606
607
608
609
609
610
611
612
613
614
615
616
617
618
619
619
620
621
622
623
624
625
626
627
628
629
629
630
631
632
633
634
635
636
637
638
639
639
640
641
642
643
644
645
646
647
648
649
649
650
651
652
653
654
655
656
657
658
659
659
660
661
662
663
664
665
666
667
668
669
669
670
671
672
673
674
675
676
677
678
679
679
680
681
682
683
684
685
686
687
688
689
689
690
691
692
693
694
695
696
697
698
699
699
700
701
702
703
704
705
706
707
708
709
709
710
711
712
713
714
715
716
717
718
719
719
720
721
722
723
724
725
726
727
728
729
729
730
731
732
733
734
735
736
737
738
739
739
740
741
742
743
744
745
746
747
748
749
749
750
751
752
753
754
755
756
757
758
759
759
760
761
762
763
764
765
766
767
768
769
769
770
771
772
773
774
775
776
777
778
779
779
780
781
782
783
784
785
786
787
788
789
789
790
791
792
793
794
795
796
797
797
798
799
799
800
801
802
803
804
805
806
807
808
809
809
810
811
812
813
814
815
816
817
818
819
819
820
821
822
823
824
825
826
827
828
829
829
830
831
832
833
834
835
836
837
838
839
839
840
841
842
843
844
845
846
847
848
849
849
850
851
852
853
854
855
856
857
858
859
859
860
861
862
863
864
865
866
867
868
869
869
870
871
872
873
874
875
876
877
878
879
879
880
881
882
883
884
885
886
887
888
889
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
909
910
911
912
913
914
915
916
917
918
919
919
920
921
922
923
924
925
926
927
928
929
929
930
931
932
933
934
935
936
937
938
939
939
940
941
942
943
944
945
946
947
948
949
949
950
951
952
953
954
955
956
957
958
959
959
960
961
962
963
964
965
966
967
968
969
969
970
971
972
973
974
975
976
977
978
979
979
980
981
982
983
984
985
986
987
988
989
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1839
1840
1841
1842
1843
1844
1845
1846
1847<br

INTRODUCTION

2 Huawei claims that the United States Attorney’s Office (the “USAO”) filed this
3 case to further a political campaign against Chinese businesses. Huawei’s claim is
4 baseless—the USAO filed this case because Huawei had engaged in a brazen corporate
5 plot to steal sensitive trade secrets in this District, and had tried to cover up its
6 misconduct by repeatedly lying about what had happened. Moreover, Huawei’s actions
7 were not isolated, or the product of a few employees. Rather, Huawei China maintained
8 a secret, formal program that rewarded employees with bonuses who stole sensitive
9 information from competitors. In addition, as a congressional investigation found,
10 Huawei has exhibited a pattern and practice of stealing intellectual property, and
11 repeatedly been dishonest when questioned about its practices and its conduct. In short,
12 Huawei is no victim of selective prosecution—its misconduct and dishonesty are why the
13 USAO opened and pursued this investigation, culminating in the charges that are
14 currently pending before the Court. Huawei fails to meet the “rigorous” standard for
15 dismissal or obtaining discovery, and therefore its motion should be denied.

BACKGROUND

A. The U.S. House of Representatives Investigation

In 2011, the U.S. House of Representatives Permanent Select Committee on Intelligence (the “House Committee” or “Committee”) launched an investigation into Huawei and ZTE, another Chinese telecommunications company. *See Exhibit A at iv.* The House Committee’s focus was the extent to which the two companies posed a risk to national security in light of their increasing sales to the United States market. *Id.* at iv, 8.

23 The House Committee began by noting that “Chinese intelligence collection
24 efforts against the U.S. government are growing in scale, intensity and sophistication.”
25 *Id.* at 2 (internal quotation omitted). The Committee stated that “U.S. private sector firms
26 and cybersecurity specialists report an ongoing onslaught of sophisticated computer
27 network intrusions that originate in China, and are almost certainly the work of, or have
28 the backing of, the Chinese government.” *Id.* The Committee found that “Chinese

1 intelligence services, as well as private companies and other entities, often recruit those
 2 with direct access to corporate networks to steal trade secrets and other sensitive
 3 proprietary data.” *Id.*

4 The House Committee concluded that Huawei and ZTE posed a unique risk to the
 5 United States because the companies provided a “wealth of opportunities for Chinese
 6 intelligence agencies to insert malicious hardware or software implants into critical
 7 telecommunications components and systems.” *Id.* at 3. The Committee noted that the
 8 Chinese government could seek the companies’ cooperation in this regard, and that both
 9 companies “would be obligated [under Chinese law] to cooperate with any request by the
 10 Chinese government to use their systems or access them for malicious purposes under the
 11 guise of state security.” *Id.*

12 During its investigation, the House Committee requested a variety of information
 13 from Huawei to better evaluate the risk that it posed. *Id.* at 9. The Committee found
 14 Huawei to be “obstructionist” in response to its requests. *Id.* at 10. Huawei refused to
 15 turn over a number of documents, and the few key documents that it did disclose were
 16 unsigned drafts that could not be authenticated. *Id.* at 9, 12, 15, 16. The Committee
 17 heard from Huawei executives, but found their answers to be “not credible,” “evasive,”
 18 “incomplete,” and “vague.” *Id.* at 10, 21, 26, 27, 32. The Committee expressed
 19 bewilderment that the executives “claimed to have no understanding or knowledge of
 20 commonly used terms, could not answer questions about the composition of [Huawei’s]
 21 internal Party Committees, refused to provide straightforward answers about [Huawei’s]
 22 operations in the United States, sought to avoid answering questions about [Huawei’s]
 23 histories of intellectual property protection, and claimed to have no understanding or
 24 knowledge of Chinese laws that force [the company] to comply with the Chinese
 25 government’s requests for access to [its] equipment.” *Id.* at 10.

26 The Committee also found that Huawei had provided a misleading and incomplete
 27 account of the company’s ties to the Chinese government. As the Committee noted,
 28 Huawei repeatedly has asserted “that it is a private, employee-owned and controlled

1 company that is not influenced by the Chinese government or Chinese Communist
 2 Party.” *Id.* at 14. However, Huawei refused to answer basic questions about its structure
 3 and history, including the identity of its largest shareholders, who had served on its Board
 4 of Directors, and how Board members were chosen. *Id.* at 14-16. Of particular concern,
 5 Huawei refused to disclose details about how it interacted with the Chinse government.
 6 *Id.* at 21-22. The Committee noted that Huawei maintained an internal Chinese
 7 Communist Party Committee, and that Huawei refused to provide details about the Party
 8 Committee’s role and connection to the government. *Id.* at 23-24. When Huawei was
 9 asked about its ties to the Chinese military, its responses were not credible. *Id.* at 24. For
 10 example, Huawei denied that its Chairwoman had been previously affiliated with the
 11 Ministry of State Security, despite the fact that Huawei’s own website listed her as
 12 having had this role. *Id.* When confronted about the discrepancy, Huawei offered no
 13 explanation. *Id.*

14 The Committee also uncovered evidence that Huawei was engaged in widespread
 15 illegal conduct. The Committee heard from “numerous sources” who revealed that
 16 Huawei had engaged in a “pattern of disregard for the intellectual property rights” of
 17 United States companies. *Id.* at 31. These sources included former employees, who said
 18 that Huawei was “known to purposely use the patented material of other firms” and
 19 pirated software. *Id.* at 31, 35. Both current and former employees also told the
 20 Committee that Huawei was engaged in numerous law violations relating to bribery,
 21 corruption, fraud, immigration, and discrimination. *Id.* at 35.

22 **B. Huawei’s Formal Bonus Program for Rewarding Theft of Intellectual
 23 Property**

24 In 2013, in the wake of the House Committee report, Huawei China launched a
 25 formal bonus program to reward employees who stole competitor information. *See*
 26 generally Indictment, Dkt. 1, ¶¶ 47-48. Under the policy, employees were told that they
 27 had the responsibility to collect competitor information. The company said that monetary
 28 awards would be available to employees who stole information, and that the amount of

1 the awards would be tied to the value of the information obtained. The company said that
 2 the “Account Dept” and a “Competition Mgmt Group” would be responsible for
 3 reviewing the information collected and awarding bonuses. The company emphasized
 4 that employees would not be “punished” for stealing information. Employees were
 5 directed to send particularly sensitive information to a special Huawei encrypted internal
 6 email address.

7 Huawei China’s directive was sent to employees based in the United States at
 8 Huawei USA. In response, Huawei USA’s human resources executive, recognizing the
 9 blatant illegality of the directive, emailed Huawei USA’s employees. She noted that
 10 employees had received an email from headquarters titled “Attention to get Rewards!”
 11 and that the email “seems to indicate that [employees] are being encouraged and could
 12 possibly earn a monetary award for collecting confidential information regarding our
 13 competitors and sending it back to HQ.” *Id.* ¶ 48. She further wrote that although the
 14 theft program “may be normal and within the usual course of business” in “some foreign
 15 countries and regions,” the program was prohibited by Huawei Device USA’s corporate
 16 policies. *Id.* Nothing in her email suggested that the policy was being suspended in
 17 China, including as to efforts by China-based employees to steal information from the
 18 United States.

19 **C. Litigation Alleging Trade Secret Theft by Huawei**

20 Prior to the events of this case, Huawei had been sued at least twice in the United
 21 States for serious allegations of trade secret theft.¹ In 2003, Cisco had sued multiple
 22 Huawei entities, alleging that Huawei had stolen Cisco’s intellectual property relating to
 23 network routers. *See Exhibit B* ¶ 1. Cisco sold, among other things, routers that handled
 24 internet and other data traffic. *Id.* ¶ 10. Huawei launched a competing router, which it
 25 marketed as a cheaper version of the Cisco router. *Id.* ¶ 12. Cisco alleged that Huawei
 26

27 ¹ Huawei also has been sued in the United States multiple times for patent violations, including a recent case that
 28 resulted in an award of over \$10 million dollars after a finding that Huawei had willfully violated multiple patents.
See Optis Wireless Technology LLC et al. v. Huawei Device USA, Inc. et al., CV17-123 (E.D. Tex.), Dkt. 374.

1 had copied Cisco's source code and other software in developing its router. *Id.* ¶¶ 15-22.
 2 Cisco showed, in particular, that whole portions of Huawei's code were line-by-line
 3 identical to Cisco's code. *Id.* ¶ 17. Cisco also alleged that Huawei had simply copied
 4 Cisco's user manual when developing the manual for its routers. *Id.* ¶¶ 23-24. In 2004,
 5 Huawei and Cisco settled the case.

6 In 2010, Motorola had sued a Huawei entity, alleging trade secret theft. *See*
 7 Exhibit C ¶ 338. According to Motorola, one of Motorola's employees repeatedly copied
 8 source code and other sensitive information from its network. *Id.* ¶ 54. The employee
 9 had been secretly working for Lemko, one of Motorola's competitors, which had offices
 10 in China. *Id.* ¶¶ 49, 53. The employee was arrested while attempting to board a flight to
 11 China with \$30,000 in cash and over 1000 electronic and paper Motorola documents in
 12 her possession. *Id.* ¶ 68. During the course of its investigation, Motorola learned that
 13 Lemko's founder had sent stolen Motorola product specifications to Huawei. *Id.* ¶ 350-
 14 54. In 2010, the case settled.

15 **D. The Underlying Case Conduct**

16 The conduct in this case, which is detailed in the Indictment, reflected a number of
 17 incredibly aggravating circumstances, particularly in light of the company's history, as
 18 outlined above.

19 *First*, Huawei China engineers, including the head of its robotics program,
 20 repeatedly pressured Huawei USA employees to steal T-Mobile's trade secret robot
 21 technology over the course of nearly a year. Indictment ¶¶ 14-23.

22 *Second*, the Huawei employees who were involved in the theft acted willfully,
 23 knowing that T-Mobile was unwilling to share its technology, and had carefully guarded
 24 it. As a senior Huawei USA employee told Huawei China engineers who were
 25 pressuring U.S.-based employees to steal additional information: “[T-Mobile] has set up
 26 a security system by putting camera into the robot Lab. I think everyone knows what this
 27 means . . . We can't provide any further information to [headquarters] because we can't
 28 get anything from [T-Mobile].” *Id.* ¶ 24.

1 *Third*, Huawei China took the extraordinary step of flying an engineer to the
 2 United States for the purpose of stealing T-Mobile's technology. *Id.* ¶ 27. When this
 3 employee was caught in T-Mobile's laboratory without authorization, he returned *the*
 4 *very next day* to continue to steal information, only to be caught a second time. *Id.* ¶ 28-
 5 29.

6 *Fourth*, after these two incidents, T-Mobile limited access to the laboratory to a
 7 single Huawei employee. *Id.* ¶ 31. Incredibly, Huawei China immediately tasked this
 8 employee with stealing additional information, culminating in his smuggling a robot arm
 9 out of the laboratory. *Id.* ¶¶ 32-34. When confronted, this employee initially lied to T-
 10 Mobile about having taken the arm—all the while giving the arm to the Chinese engineer
 11 who had been kicked out the laboratory to share with his colleagues in China. *Id.* ¶¶ 34-
 12 35.

13 *Fifth*, after T-Mobile learned of the robot arm theft, Huawei prepared a bogus
 14 "investigation report." *Id.* ¶ 39. Much like how the company had responded to Congress,
 15 the report was riddled with misstatements and material omissions. *Id.* As just one
 16 example, the report said that the Chinese engineer had taken nine photographs in a
 17 "moment of indiscretion," failing to point out that the engineer had been sent to the
 18 United States *for the purpose* of stealing T-Mobile's technology, that his actions were the
 19 culmination of a months-long campaign involving numerous employees to steal the
 20 technology, and that multiple employees had taken unauthorized photographs in the
 21 laboratory on several prior occasions. *Id.* ¶ 42.

22 **E. The Timeline of this Prosecution**

23 As Huawei acknowledges in its motion, T-Mobile reported Huawei's theft of its
 24 trade secrets to the Seattle FBI in August 2013, weeks after it discovered Huawei's
 25 criminal activities. The events at issue became the subject of a civil lawsuit, filed by T-
 26 Mobile in September 2014, and litigated through a jury trial in April and May 2017, with
 27 post-trial litigation thereafter. Along the way, the Seattle FBI referred the case to the
 28 USAO. By December 2017—less than seven months after the verdict in the civil case —

1 the Assistant United States Attorneys handling this case had contact with defense counsel
 2 for Huawei and advised that the USAO planned to seek an indictment against Huawei in
 3 the coming months. The USAO and defense counsel maintained regular contact about
 4 the case throughout 2018 and into early January 2019, at which point the Grand Jury
 5 returned the Indictment in this case.

6 **ARGUMENT**

7 **I. HUAWEI HAS WHOLLY FAILED TO MEET ITS HIGH BURDEN**
 8 **IN SHOWING SELECTIVE PROSECUTION.**

9 **A. The Rigorous Standard for Evaluating Selective Prosecution Claims**

10 “In our criminal justice system, the Government retains ‘broad discretion’ as to
 11 whom to prosecute.” *Wayte v. United States*, 470 U.S. 598, 607 (1985) (quoting *United*
 12 *States v. Goodwin*, 457 U.S. 368, 380, n.11 (1982)). “[S]o long as the prosecutor has
 13 probable cause to believe that the accused committed an offense defined by statute, the
 14 decision whether or not to prosecute, and what charge to file or bring before a grand jury,
 15 generally rests entirely in his [or her] discretion.” *Bordenkircher v. Hayes*, 434 U.S. 357,
 16 364 (1978); *see also United States v. Arenas-Ortiz*, 339 F.3d 1066, 1068 (9th Cir. 2003)
 17 (“We must exercise a high degree of deference to the decision of prosecuting authorities
 18 to bring charges, because the Constitution assigns that decision to the executive branch of
 19 government.”). “This broad discretion rests largely on the recognition that the decision to
 20 prosecute is particularly ill-suited to judicial review.” *Wayte*, 470 U.S. at 607. “Such
 21 factors as the strength of the case, the prosecution’s general deterrence value, the
 22 Government’s enforcement priorities, and the case’s relationship to the Government’s
 23 overall enforcement plan are not readily susceptible to the kind of analysis the courts are
 24 competent to undertake.” *Id.* In addition, as the Supreme Court has recognized:

25 [Judicial review of charging decisions] entails systemic costs of particular
 26 concern. Examining the basis of a prosecution delays the criminal
 27 proceeding, threatens to chill law enforcement by subjecting the
 28 prosecutor’s motives and decisionmaking to outside inquiry, and may
 undermine prosecutorial effectiveness by revealing the Government’s

1 enforcement policy. All these are substantial concerns that make the courts
 2 properly hesitant to examine the decision whether to prosecute.

3 *Id.*

4 The doctrine of “selective prosecution” is a narrow exception to the general rule
 5 that a prosecutor’s charging decisions are immune from judicial review. *See generally*
 6 *United States v. Armstrong*, 517 U.S. 456 (1996). Under the selective prosecution
 7 doctrine, a prosecutor cannot base his or her charging decision upon an “unjustifiable
 8 standard such as race, religion, or other arbitrary classification.” *Id.* at 464 (quoting
 9 *Oyler v. Boles*, 368 U.S. 448, 456 (1962)). However, because “[t]he presumption of
 10 regularity supports’ prosecutorial decisions,” the defendant bears a heavy burden in
 11 showing selective prosecution. *United States v. Armstrong*, 517 U.S. 456, 464 (1996)
 12 (quoting *United States v. Chemical Foundation, Inc.*, 272 U.S. 1, 14–15 (1926)).
 13 Specifically, the defendant must make two showings. First, a defendant must establish
 14 that similarly situated individuals of a different race, or in this case, national origin, were
 15 not prosecuted. *See United States v. Arenas-Ortiz*, 339 F.3d 1066, 1068 (9th Cir. 2003).
 16 “This standard . . . is ‘a demanding one.’” *Id.* (quoting *Armstrong*, 517 U.S. at 463)). In
 17 addition, it is not enough to show that a large number of individuals or a certain race or
 18 national origin have been prosecuted for a particular offense—rather, the defendant must
 19 show that individuals of other races or national origins “had been left unprosecuted.”
 20 *United States v. Turner*, 104 F.3d 1180, 1185 (9th Cir. 1997). Second, the defendant
 21 must show that the prosecution was “based on an impermissible motive.” *United States*
 22 *v. Bourgeois*, 964 F.2d 935, 938 (9th Cir. 1992); *see also Armstrong*, 517 U.S. at 465.

23 The standard for obtaining discovery in support of a selective prosecution claim
 24 also is high. *Armstrong*, 517 U.S. at 468. As the Supreme Court has stated: “The
 25 justifications for a rigorous standard for the elements of a selective prosecution claim . . .
 26 require a correspondingly rigorous standard for discovery in the aid of such a claim.” *Id.*
 27 In order to obtain discovery, “defendant must produce ‘some evidence that similarly
 28 situated defendants of other races [or national origins] could have been prosecuted, but

1 “were not.”” *United States v. Arenas-Ortiz*, 339 F.3d 1066, 1069 (9th Cir. 2003) (quoting
 2 *Armstrong*, 517 U.S. at 469). Although the standard for obtaining discovery is less than
 3 the standard for establishing an actual violation, “[e]ven [the discovery] standard . . . is a
 4 ‘rigorous’ one designed to minimize interference with the prosecutorial function.” *Id.*
 5 (quoting *Armstrong*, 517 U.S. at 468).

6 As set forth below, Huawei has wholly failed to meet either prong of the selective
 7 prosecution doctrine, and is not entitled to discovery, let alone dismissal of this action.

8 **B. Huawei Has Not Established That Similarly Situated Actors Were Not
 9 Prosecuted.**

10 Huawei has completely failed to show that similarly situated actors could have
 11 been prosecuted, but were not. *Armstrong*, 517 U.S. at 469. Huawei is literally in a class
 12 by itself—its history of a flagrant disregard for the rule of law is virtually unmatched
 13 compared to any company that purports to conduct legitimate business. To summarize:

- 14 • As a congressional investigation found, Huawei had exhibited a “pattern of
 15 disregard for the intellectual property rights” of United States companies, and was
 16 engaged in widespread illegal conduct pertaining to bribery, corruption, fraud,
 17 immigration, and discrimination. *See Exhibit A* at 31, 35.

- 18 • Huawei executives repeatedly lied during the congressional investigation
 19 and concealed material facts. *See Exhibit A* at 9, 10, 12, 14, 16, 21, 26, 27, 32.

- 20 • Huawei has been sued twice for serious allegations of trade secret and
 21 related theft. *See Exhibits B, C.* In both cases, the plaintiffs came forward with
 22 compelling evidence that Huawei had illegally misappropriated trade secrets and
 23 protected information.

- 24 • In this case, Huawei was caught red-handed, having engaged in a months-
 25 long corporate campaign to steal T-Mobile’s sensitive trade secrets. Supervisors in China
 26 directed that the theft campaign continue even after one of its employees had been caught
 27 sneaking into the laboratory twice without permission to access the sensitive technology.
 28 When a second employee was caught smuggling a part out of the laboratory, the

1 company sent T-Mobile a false and misleading report about what had happened that
 2 contained numerous misstatements and material omissions.

3 • In the wake of the theft, Huawei China launched a formal program directing
 4 its employees to steal competitor information, with the promise of monetary awards tied
 5 to the sensitivity and value of the information stolen. Astoundingly, at the very same
 6 time the Huawei “investigation report” attempted to mislead T-Mobile into believing that
 7 the theft was the act of two rogue employees, Huawei China was advancing a corporate-
 8 wide program encouraging corporate espionage and theft. Huawei did not disclose this
 9 program to T-Mobile as part of the company’s “investigative report” or at any point
 10 during the ensuing civil litigation.

11 In the face of this extraordinary history,² Huawei points to three civil cases as
 12 evidence that similarly situated actors have not been prosecuted:

13 • *Epic Systems Corporation v. Tata Consultancy Services, Ltd. et al.*, No. 14-
 14 CV-748 (W.D. Wis. Oct. 31, 2014). The plaintiff, Epic Systems, alleged that the
 15 defendant, Tata Consultancy Services, had misappropriated its software for the purpose
 16 of designing competing software. The jury found for Epic and awarded \$700,000,000 in
 17 punitive damages, and \$240,000,000 in compensatory damages, but the Court later
 18 reduced the total award to \$420,000,000.

19 • *Wellogix Inc. v. BP America Inc. et al.*, 3:08-CV-00119 (S.D. Tex. May 16,
 20 2008). Wellogix claimed that three companies misappropriated its software. The district
 21 court dismissed the case as to one of the defendants, and another proceeded to arbitration,
 22 resulting in a mixed decision. *See Wellogix, Inc. v. Accenture, LLP*, 716 F.3d 867, 874
 23 (5th Cir. 2013). Wellogix proceeded against the third defendant, and prevailed, obtaining
 24

25
 26 ² Huawei brazenly suggests that prosecution is not supported by the Justice Manual, which sets forth a non-
 27 exhaustive list of “discretionary factors” that prosecutors consider in deciding whether to bring a trade secrets or
 28 foreign economic espionage charge. *See* Justice Manual § 9-59.100, available at <https://www.justice.gov/jm/jm-9-59000-economic-espionage>. Those factors include consideration of the “scope of the criminal activity.” *Id.* This factor alone strongly supported prosecution, given all of the aggravating circumstances of the offense, as outlined above.

1 an award of \$26.2 million in compensatory damages and \$18.2 million in punitive
 2 damages.

3 • *CardiAQ Valve Technologies, Inc. v. Neovasc Inc. et al.*, No. 14-CV-12405
 4 (D. Mass. June 6, 2014). The plaintiff alleged that the defendant had misappropriated its
 5 heart valve technology in developing its own product. The jury awarded \$70 million,
 6 which the judge later enhanced to \$91 million.

7 Many of the substantive filings in these cases are sealed, and thus it is impossible
 8 to identify all of the differences in the cases compared to the case at bar. In particular, in
 9 the absence of the complete case records, it is impossible to evaluate the strength of the
 10 cases, including whether they were provable beyond a reasonable doubt. *See, e.g.,*
 11 *United States v. Mathur*, No. 2:11-CR-00312-MMD, 2012 WL 3135548, at *5
 12 (D. Nev. June 8, 2012) (defendant failed to meet burden where, among other things, he
 13 cited cases purporting to involve similar conduct without analysis of the “evidence,
 14 investigation, level of cooperation, or the decision-making process in any of the cases”),
 15 *report and recommendation adopted*, No. 2:11-CR-00312-MMD, 2012 WL 3135532
 16 (D. Nev. Aug. 1, 2012).

17 Nonetheless, even in the absence of the full records, it is clear that the cases are
 18 significantly different compared to this case. Most importantly, there was no suggestion
 19 that the civil defendants had any history remotely resembling the long history of
 20 wrongdoing of Huawei. *See United States v. Smith*, 231 F.3d 800, 812 (11th Cir. 2000)
 21 (in context of selective prosecution: “The government can legitimately place a higher
 22 priority on prosecuting someone who commits an offense three, six or seven times, than
 23 someone who commits an offense once or twice, especially when the offense is a non-
 24 violent one.”); *United States v. Lewis*, 517 F.3d 20, 28 (1st Cir. 2008) (same). There
 25 certainly was no suggestion that any of the civil defendants had the same formal program
 26 of theft and bonuses that Huawei China had implemented even after the thefts in this
 27 case. Moreover, there was no suggestion that the civil defendants had tried to dupe the
 28 plaintiff through a false and misleading investigation report. In these circumstances, the

1 civil cases are not similarly situated with this case. *See, e.g., United States v. Estrada-*
 2 *Plata*, 57 F.3d 757, 761 (9th Cir. 1995) (rejecting selective prosecution claim by noting
 3 that defendants' conduct was more egregious in nature compared to others who had
 4 committed the same offense); *United States v. Sutcliffe*, 505 F.3d 944, 954
 5 (9th Cir. 2007); *United States v. Walli*, No. 3:12-CR-107, 2013 WL 1773617, at *11
 6 (E.D. Tenn. Mar. 11, 2013).

7 Even if these three cases presented substantially similar circumstances—which
 8 they do not—the small number of cases identified by Huawei—*three in a six-year span*—
 9 dooms its claim. As courts have recognized, a defendant typically must provide evidence
 10 of more than a few similarly situated persons because there always will be examples
 11 where deserving individuals escape prosecution for a variety of innocuous reasons,
 12 including the lack of a criminal referral to law enforcement or limited resources. *United*
 13 *States v. Tibbetts*, 646 F.2d 193, 195-96 (5th Cir. 1981) (finding no selective prosecution
 14 of a tax protestor partly because: “Due to limited resources of the government, there will
 15 always be some tax evaders and tax protestors who elude prosecution by the government.
 16 This factor is not sufficient to show selective prosecution.”); *United States v. Johnson*,
 17 577 F.2d 1304, 1308-09 (5th Cir. 1978); *United States v. Brewer*, 681 F.2d 973, 975 (5th
 18 Cir. 1982) (same); *United States v. Hayes*, 589 F.2d 811, 819 & 819 n.4 (5th Cir. 1979)
 19 (finding that defendant failed to satisfy first prong of the selective prosecution test
 20 because he only presented evidence of three other cases in which there was no federal
 21 prosecution after a state prosecution had been pursued in good faith).

22 In addition, Huawei claims that it cannot find another example of a criminal case
 23 brought against a defendant who lost a civil trade secrets case in the absence of a finding
 24 of willfulness. Huawei seems to assume that its conduct was not willful—quite the
 25 contrary, there is overwhelming evidence that Huawei deliberately targeted T-Mobile's
 26
 27
 28

1 technology, knowing that what it was doing was wrong.³ Indeed, Huawei’s efforts to
 2 mislead T-Mobile through the bogus investigation report only confirm the company’s bad
 3 intent.

4 Finally, having failed to identify similarly situated defendants who were not
 5 prosecuted, Huawei instead focuses on the relatively large number of Chinese defendants
 6 who have been prosecuted for trade secret theft. Huawei, however, misunderstands its
 7 burden: in order to prevail on a selective prosecution claim, a defendant must establish
 8 that similarly situated individuals of a different national origin were not prosecuted. *See*
 9 *United States v. Arenas-Ortiz*, 339 F.3d 1066, 1068 (9th Cir. 2003). Huawei has not done
 10 so. Moreover, given Congressional and Executive findings that the Chinese government
 11 has systematically encouraged and enlisted individuals to steal intellectual property from
 12 the United States, it hardly is surprising that a large number of Chinese defendants have
 13 been prosecuted. These prosecutions do not reflect any improper bias or motive—but
 14 rather a response to an identified threat targeting the United States.

15 In sum, Huawei has wholly failed to show that similarly situated actors could have
 16 been prosecuted but were not. Thus, its selective prosecution claim, including its request
 17 for discovery, fails.

18 //

19 //

20 _____

21 ³³ Huawei asserts that the civil jury found that Huawei had not engaged in any “willful *or* malicious conduct,”
 22 Motion at 2 (emphasis added). Although it is true that the jury found that Huawei had not engaged in “willful *and*
 23 malicious” conduct, that phrase was defined extremely narrowly in the jury instructions. *See T-Mobile USA, Inc. v.*
Huawei Device USA, Inc., 14-CV-13551 (W.D. Wash.), Dkt. 484 at 2. Specifically, the jury was instructed that it
 24 had to find that Huawei acted for the *purpose* of injuring T-Mobile, or otherwise out of ill will or spite directed at T-
 25 Mobile. *See id.* Dkt. 474 at 35. Under this definition of the term “willful and malicious” conduct, it may have been
 26 reasonable for the jury to conclude that Huawei’s conduct did not qualify, because Huawei did not steal T-Mobile’s
 27 technology for the express purpose of inflicting harm on T-Mobile. Rather, Huawei acted to gain an unfair
 28 advantage for themselves by obtaining technology without having to develop or pay for it, with total disregard for
 the resultant collateral harm that would befall T-Mobile. Although this motive on Huawei’s behalf would not have
 met the Court’s definition of “willful and malicious” conduct in the civil case, Huawei’s conduct was nonetheless
 clearly deliberate and aggravating, and weighed in favor of criminal prosecution. Moreover, unlike in the civil
 context, a violation of 18 U.S.C. § 1832 requires only that Huawei act knowing that its conduct would harm T-
 Mobile, and not for that express purpose. *See id.* § 1832(a)(statute requires proof merely that defendant knew that
 the theft would harm the victim).

1 **C. The USAO Did Not File This Case For an Impermissible Motive**

2 Huawei fares no better under the second prong. Huawei baldly asserts that this
 3 prosecution was filed for the impermissible purpose of “secur[ing] leverage in trade
 4 negotiations” with China and otherwise as part of an illegitimate campaign against
 5 Chinese businesses. Motion at 12. Huawei is wrong—this action was filed for all of the
 6 reasons stated above—Huawei is a recidivist thief of intellectual property that was caught
 7 red-handed, tried to cover it up, and then implemented a formal program directing its
 8 employees to continue stealing information from competitors. In support of its wild
 9 assertions regarding prosecutorial motive, Huawei makes a number of claims, none of
 10 which withstand scrutiny.

11 **1. The China Initiative**

12 Huawei spends a large portion of its motion complaining about the Department of
 13 Justice’s China Initiative. This initiative grew out of the same concerns that Congress
 14 identified in the 2012 House Report—that the Chinese government is engaged in a
 15 widespread campaign of intellectual property theft against the United States.⁴ In light of
 16 this concern, the Department of Justice is prioritizing Chinese economic espionage cases,
 17 and taking other steps to minimize the threat posed by the Chinese government, such as
 18 by conducting business outreach.⁵ The Department of Justice is not prioritizing these
 19 cases because the defendants are Chinese; rather, the Department is prioritizing them in
 20 response to a specifically identified threat targeting United States intellectual property.
 21 The Department’s China Initiative is thus not discriminatory—but rather an appropriate
 22 response to threatening conduct by a foreign actor directed at the United States.

23 The United States District for the District of Columbia’s decision in *United States*
 24 *v. Concord Management & Consulting LLC*, 18CR-32 (Oct. 16, 2018) (attached as
 25 Exhibit D) demonstrates this point. In that case, a Russian corporation was charged by

26
 27 ⁴ <https://www.justice.gov/opa/speech/attorney-general-jeff-sessions-announces-new-initiative-combat-chinese-economic-esionage> (visited August 9, 2019).

28 ⁵ *Id.*

1 the Special Counsel for its role in the Russian government’s interference with the 2016
 2 election. *Id.* at 2. The Russian corporation complained that it was a victim of selective
 3 prosecution because the Special Counsel’s mandate was to examine cases involving the
 4 Russian government, and therefore was focused on individuals and corporations of a
 5 particular national origin. *Id.* at 3. The court rejected this claim, noting that “the Special
 6 Counsel is prosecuting individuals and entities because of their involvement in the
 7 Russian government’s efforts to interfere in the 2016 presidential election—not because
 8 of their Russian nationality.” *Id.* at 3 (internal quotation and citation omitted).

9 More broadly, Huawei’s reliance on the China Initiative is totally misplaced
 10 because the initiative was launched *well after* a decision had already been made to charge
 11 Huawei in this case. Specifically, the Attorney General launched the initiative on
 12 November 1, 2018. However, as noted above, the USAO informed defense counsel of its
 13 intention to seek an indictment against Huawei in December 2017. Thus, the China
 14 Initiative did not serve as the grounds for why this prosecution was brought.

15 Finally, in various places in its brief, Huawei seeks to cast doubt on the notion that
 16 the Chinese government poses the threat to intellectual property that the United States
 17 Government says it does. Huawei’s aspersions of the collective judgment of Congress
 18 and the Executive about the risks posed by the Chinese government should be
 19 disregarded by the Court. Not only has Huawei offered nothing in support of its
 20 contentions, but, more fundamentally, this Court is not the proper forum to evaluate the
 21 security risks posed by a foreign government. *See Holder v. Humanitarian Law Project*,
 22 561 U.S. 1, 33-34 (2010) (deference to the political branches is particularly appropriate
 23 with respect to national security and foreign affairs, given the relative institutional
 24 capacity, informational access, and expertise of the courts); *Reno v. American-Arab
 25 Anti-Discrimination Comm.*, 525 U.S. 471, 49 (1999) (explaining that even if the
 26 Executive “disclose[d] its … reasons for deeming nationals of a particular country a
 27 special threat,” courts would be “unable to assess their adequacy”).

1 **2. The Timing of the Prosecution**

2 Huawei separately points to the fact that the Indictment was unsealed in
 3 January 2019—days after trade talks with China were cancelled, and in the midst of the
 4 current trade dispute with China—as purported evidence that this case was brought for
 5 political purposes. Motion at 2-3. Huawei seems to be imagining a scenario under which
 6 the President, on his way out of the negotiation room, ordered the USAO to obtain the
 7 Indictment in this case. Nothing could be further from the truth. As noted above, the
 8 USAO made its own independent decision to pursue an indictment in this case, and
 9 communicated its intentions to do so to counsel for Huawei in December 2017—well in
 10 advance of the current trade dispute with China.

11 The precise timing of the Indictment is of no mystery to Huawei. The parties
 12 entered into a statute of limitations tolling agreement that was set to expire in
 13 January 2019, and the government asked the Grand Jury to return an indictment prior to
 14 that time. In sum, the timing of the Indictment in no way supports Huawei’s assertion
 15 that this case was filed to obtain some sort of political leverage.

16 **3. The Civil Jury’s Verdict**

17 Huawei also claims to profess bewilderment that this case was brought “after a
 18 civil jury awarded *zero* damages,” claiming that no valid criminal prosecution would be
 19 sought in these circumstances. Motion at 12 (emphasis in original). The jury, in fact,
 20 awarded \$4.8 *million* dollars in unjust enrichment damages, not zero. Dkt. 484 at 3. In
 21 addition, the jury’s decision was undoubtedly influenced by the fact that Huawei was
 22 caught before it could fully reverse engineer and implement T-Mobile’s technology. Had
 23 Huawei not been caught, T-Mobile would have suffered greater harm, and therefore been
 24 entitled to a greater amount of damages. In addition to the actual and potential harm
 25 suffered by T-Mobile, Huawei’s history, outlined above, more than served as a
 26 compelling basis for criminal charges in this case.

1 **4. Other Executive Actions Targeting Huawei**

2 Huawei also complains about other Executive actions targeting Huawei, namely
 3 the decision by the Department of Commerce to restrict the export of American goods
 4 and technology to Huawei without a license. These actions are not before the Court.⁶
 5 The only question is whether Huawei has shown that *this prosecution* was the product of
 6 bad faith selective prosecution. For all of the reasons stated above, Huawei has fallen far
 7 short in making this showing. In addition, given Huawei's tortured history, including,
 8 most notably, the findings of the 2012 House Report, it hardly is surprising that it is the
 9 subject of other Executive actions. But, regardless of the merit of those actions, this
 10 action was brought for entirely appropriate and understandable reasons. Thus, its motion
 11 should be denied.

12 **D. Huawei Is Not Entitled to Discovery in Support of its Failed Claim**

13 As outlined above, Huawei has not met the "rigorous" standard for obtaining
 14 discovery, given its complete failure to identify similarly-situated actors who were not
 15 prosecuted, along with its general failure to meet either prong of the selective prosecution
 16 standard. *United States v. Arenas-Ortiz*, 339 F.3d 1066, 1069 (9th Cir. 2003) (standard
 17 for selective prosecution standard is a 'rigorous' one designed to minimize interference
 18 with the prosecutorial function.") (quoting *Armstrong*, 517 U.S. at 468). In addition,
 19 Huawei's discovery requests are wildly overbroad, pertaining to numerous topics totally
 20 unrelated to this prosecution, and even seeking documents in the possession of Congress.
 21 See Defense Request No. 24, Exhibit A to Def. Motion at 6 (demanding "[a]ll documents
 22 or information" relating to objections from the Committee on Foreign Investment in the
 23 United States about Broadcom's takeover of Qualcomm); Defense Request No. 11, *id.* at
 24 5 (All "documents relating to the reputation of Huawei."); Defense Request No. 26, *id.* at
 25
 26

27 ⁶ Huawei cites comments that President Trump made about potentially reaching a compromise on the Department of
 28 Commerce sanctions and the case against Huawei's CFO, Meng Wanzhou, who is charged in the Eastern District of
 New York for conduct unrelated to this case. None of the comments pertain to this action, and therefore they are
 irrelevant.

1 6 (All “documents or information” related to Congress’s inclusion of Huawei and its
2 competitor, ZTE, in the National Defense Authorization Act.); Defense Request No. 13,
3 *id.* at 5 (All “documents and communications, received, prepared or created” by “any
4 Congressional committees or subcommittees in connection with any investigations in
5 Huawei.”); Defense Request No. 27, *id.* at 6 (“All documents or information” related to
6 the China Initiative, which, as described above, was launched well after a decision to
7 indict Huawei had been made.).

8 Huawei has not met its burden for discovery. Its request for discovery, as with its
9 request for dismissal, should be denied.

DATED this 22nd day of August, 2019.

Respectfully submitted,

TESSA M. GORMAN
First Assistant United States Attorney
(Acting Under Authority Conferred by
28 U.S.C. § 515)

s/ Todd Greenberg
TODD GREENBERG
THOMAS WOODS
SIDDHARTH VELAMOOR
Assistant United States Attorneys
700 Stewart Street, Suite 5220
Seattle, WA 98101-1271

1 CERTIFICATE OF SERVICE

2 I hereby certify that on August 22, 2019 I electronically filed the foregoing with
3 the Clerk of the Court using the CM/ECF system which will send notification of such
4 filing to the attorney(s) of record for the defendant(s).

5
6 *s/Jenny Fingles* _____
7 JENNY FINGLES
8 Legal Assistant
9 United States Attorney's Office
10 700 Stewart, Suite 5220
11 Seattle, Washington 98101-1271
12 Phone: 206-553-7970
13 E-mail: jenny.fingles@usdoj.gov

EXHIBIT A



Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE

A report by Chairman Mike Rogers and Ranking Member C.A. Dutch Ruppersberger of the Permanent Select Committee on Intelligence

U.S. House of Representatives
112th Congress
October 8, 2012

Contents

Executive Summary	iv
Report.....	1
I. The threat posed to U.S. national-security interests by vulnerabilities in the telecommunications supply chain is an increasing priority given the country's reliance on interdependent critical infrastructure systems; the range of threats these systems face; the rise in cyber espionage; and the growing dependence all consumers have on a small group of equipment providers.	1
A. China has the means, opportunity, and motive to use telecommunications companies for malicious purposes.	2
B. Suggested "mitigation measures" cannot fully address the threat posed by Chinese telecommunications companies providing equipment and services to United States critical infrastructure.	4
II. Investigation	7
A. Scope of Investigation	7
B. Investigative Process	8
C. Investigative Challenges.....	10
III. Summary of Findings	11
A. The Committee finds that Huawei did not fully cooperate with the investigation and was unwilling to explain its relationship with the Chinese government or Chinese Communist Party, while credible evidence exists that Huawei fails to comply with U.S. laws.....	12
i. Huawei did not provide clear and complete information on its corporate structure and decision-making processes, likely remains dependent on the Chinese government for support.....	13
ii. Huawei failed to explain its relationships with the Chinese government, and its assertions denying support by the Chinese government are not credible.....	21
iii. Huawei admits that the Chinese Communist Party maintains a Party Committee within the company, but it failed to explain what the Party	

Committee does on behalf of the Party or which individuals compose the Committee.....	22
iv. Huawei's corporate history suggests ties to the military, and Huawei failed to provide detailed answers to questions about those connections.	24
v. Huawei's failure to provide information about the Chinese government's 1999 investigation of the company for tax fraud exemplifies a company that refuses to be transparent; the apparent ease with which Huawei ended the investigation undermines Huawei's assertion that the Chinese government finds Huawei to be a disfavored telecommunications solutions provider in China.	25
vi. Huawei failed to explain its relationships with western consulting firms, and any claims that its success is on account of those relationships, rather than support by the Chinese government, are not credible.	26
vii. Huawei failed to answer key questions or provide supporting documentation for its claims to be financially independent of the Chinese government.	27
viii. Huawei failed to provide sufficient details or supporting documentation on its operations, financing, and management in the United States, undermining its claims of being a completely independent subsidiary of Huawei's parent company in Shenzhen, China.	29
ix. Evidence shows that Huawei exhibits a pattern of disregard for the intellectual property rights of other entities and companies in the United States.	31
x. Huawei failed to provide details of its operations in Iran, though it denied doing business with the government of Iran, and did not provide evidence to support its claims that it complies with all international sanctions or U.S. export laws.....	32
xi. Huawei refused to provide details on its R&D programs, and other documents undermine its claim that Huawei provides no R&D for the Chinese military or intelligence services.	33
xii. Former and current Huawei employees provided evidence of a pattern and practice of potentially illegal behavior by Huawei officials.....	34

B. ZTE failed to answer key questions or provide supporting documentation supporting its assertions; instead, it asserted that answering the Committee's requests about its internal corporate activities would leave the company criminally liable under China's states-secrets laws.....	35
i. ZTE did not alleviate Committee concerns about the control of Chinese state-owned enterprises in ZTE's business decisions and operations.	37
ii. ZTE maintains a Chinese Party Committee within the company, but has not fully clarified how the Party Committee functions, who chooses its members, and what relationship it has with the larger Chinese Communist Party.	40
iii. ZTE failed to disclose information about its activities in the U.S.	42
iv. ZTE failed to provide any answers or evidence about its compliance with intellectual property or U.S. export-control laws.....	42
v. ZTE failed to provide clear answers to Committee questions about its R&D activities, particularly as they relate to any military or government projects.....	43
Conclusion and Recommendations	44

House Permanent Select Committee on Intelligence

Chairman and Ranking Member Investigative Report on

**The U.S. National Security Issues Posed by Chinese
Telecommunications Companies Huawei and ZTE**

Executive Summary

In February 2011, Huawei Technologies Company, the leading Chinese telecommunications equipment manufacturer, published an open letter to the U.S. Government denying security concerns with the company or its equipment, and requesting a full investigation into its corporate operations.¹ Huawei apparently believed – correctly – that without a full investigation into its corporate activities, the United States could not trust its equipment and services in U.S. telecommunications networks.²

The House Permanent Select Committee on Intelligence (herein referred to as “the Committee”) initiated this investigation in November 2011 to inquire into the counterintelligence and security threat posed by Chinese telecommunications companies doing business in the United States. Prior to initiating the formal investigation, the Committee performed a preliminary review of the issue, which confirmed significant gaps in available information about the Chinese telecommunications sector, the histories and operations of specific companies operating in the United States, and those companies’ potential ties to the Chinese state. Most importantly, that preliminary review highlighted the potential security threat posed by Chinese telecommunications companies with potential ties to the Chinese government or military. In particular, to the extent these companies are influenced by the state, or provide Chinese intelligence services access to telecommunication networks, the opportunity exists for further economic and foreign espionage by a foreign nation-state already known to be a major perpetrator of cyber espionage.

As many other countries show through their actions, the Committee believes the telecommunications sector plays a critical role in the safety and security of our nation, and is thus a target of foreign intelligence services. The

Committee's formal investigation focused on Huawei and ZTE, the top two Chinese telecommunications equipment manufacturers, as they seek to market their equipment to U.S. telecommunications infrastructure. The Committee's main goal was to better understand the level of risk posed to the United States as these companies hope to expand in the United States. To evaluate the threat, the investigation involved two distinct yet connected parts: (1) a review of open-source information on the companies' histories, operations, financial information, and potential ties to the Chinese government or Chinese Communist Party; and (2) a review of classified information, including a review of programs and efforts of the U.S. Intelligence Community (IC) to ascertain whether the IC is appropriately prioritizing and resourced for supply chain risk evaluation.³

Despite hours of interviews, extensive and repeated document requests, a review of open-source information, and an open hearing with witnesses from both companies, the Committee remains unsatisfied with the level of cooperation and candor provided by each company. Neither company was willing to provide sufficient evidence to ameliorate the Committee's concerns. Neither company was forthcoming with detailed information about its formal relationships or regulatory interaction with Chinese authorities. Neither company provided specific details about the precise role of each company's Chinese Communist Party Committee. Furthermore, neither company provided detailed information about its operations in the United States. Huawei, in particular, failed to provide thorough information about its corporate structure, history, ownership, operations, financial arrangements, or management. Most importantly, neither company provided sufficient internal documentation or other evidence to support the limited answers they did provide to Committee investigators.

During the investigation, the Committee received information from industry experts and current and former Huawei employees suggesting that Huawei, in particular, may be violating United States laws. These allegations describe a company that has not followed United States legal obligations or international standards of business behavior. The Committee will be referring these allegations to Executive Branch agencies for further review, including possible investigation.

In sum, the Committee finds that the companies failed to provide evidence that would satisfy any fair and full investigation. Although this alone does not prove wrongdoing, it factors into the Committee's conclusions below. Further, this report contains a classified annex, which also adds to the Committee's concerns about the risk to the United States. The investigation concludes that the risks associated with Huawei's and ZTE's provision of equipment to U.S. critical infrastructure could undermine core U.S. national-security interests.

Based on this investigation, the Committee provides the following recommendations:

Recommendation 1: The United States should view with suspicion the continued penetration of the U.S. telecommunications market by Chinese telecommunications companies.

- The United States Intelligence Community (IC) must remain vigilant and focused on this threat. The IC should actively seek to keep cleared private sector actors as informed of the threat as possible.
- The Committee on Foreign Investment in the United States (CFIUS) must block acquisitions, takeovers, or mergers involving Huawei and ZTE given the threat to U.S. national security interests. Legislative proposals seeking to expand CFIUS to include purchasing agreements should receive thorough consideration by relevant Congressional committees.
- U.S. government systems, particularly sensitive systems, should not include Huawei or ZTE equipment, including component parts. Similarly, government contractors – particularly those working on contracts for sensitive U.S. programs – should exclude ZTE or Huawei equipment in their systems.

Recommendation 2: Private-sector entities in the United States are strongly encouraged to consider the long-term security risks associated with doing business with either ZTE or Huawei for equipment or services. U.S. network providers and systems developers are strongly encouraged to seek other vendors for their projects. Based on available classified and unclassified information, Huawei and

ZTE cannot be trusted to be free of foreign state influence and thus pose a security threat to the United States and to our systems.

Recommendation 3: Committees of jurisdiction within the U.S. Congress and enforcement agencies within the Executive Branch should investigate the unfair trade practices of the Chinese telecommunications sector, paying particular attention to China's continued financial support for key companies.

Recommendation 4: Chinese companies should quickly become more open and transparent, including listing on a western stock exchange with advanced transparency requirements, offering more consistent review by independent third-party evaluators of their financial information and cyber-security processes, complying with U.S. legal standards of information and evidentiary production, and obeying all intellectual-property laws and standards. Huawei, in particular, must become more transparent and responsive to U.S. legal obligations.

Recommendation 5: Committees of jurisdiction in the U.S. Congress should consider potential legislation to better address the risk posed by telecommunications companies with nation-state ties or otherwise not clearly trusted to build critical infrastructure. Such legislation could include increasing information sharing among private sector entities, and an expanded role for the CFIUS process to include purchasing agreements.

Report

I. The threat posed to U.S. national-security interests by vulnerabilities in the telecommunications supply chain is an increasing priority given: the country's reliance on interdependent critical infrastructure systems; the range of threats these systems face; the rise in cyber espionage; and the growing dependence all consumers have on a small group of equipment providers.

The United States' critical infrastructure, and in particular its telecommunications networks, depend on trust and reliability. Telecommunications networks are vulnerable to malicious and evolving intrusions or disruptive activities. A sufficient level of trust, therefore, with both the provider of the equipment and those performing managed services must exist at all times. A company providing such equipment, and particularly any company having access to or detailed knowledge of the infrastructures' architectural blueprints, must be trusted to comply with United States laws, policies, and standards. If it cannot be trusted, then the United States and others should question whether the company should operate within the networks of our critical infrastructure.

The risk posed to U.S. national-security and economic interests by cyber-threats is an undeniable priority. First, the country's reliance on telecommunications infrastructure includes more than consumers' use of computer systems. Rather, multiple critical infrastructure systems depend on information transmission through telecommunications systems. These modern critical infrastructures include electric power grids; banking and finance systems; natural gas, oil, and water systems; and rail and shipping channels; each of which depend on computerized control systems. Further, system interdependencies among these critical infrastructures greatly increase the risk that failure in one system will cause failures or disruptions in multiple critical infrastructure systems.⁴ Therefore, a disruption in telecommunication networks can have devastating effects on all aspects of modern American living, causing shortages and stoppages that ripple throughout society.

Second, the security vulnerabilities that come along with this dependence are quite broad, and range from insider threats⁵ to cyber espionage and attacks from sophisticated nation states. In fact, there is a growing recognition of vulnerabilities resulting from foreign-sourced telecommunications supply chains used for U.S. national-security applications. The FBI, for example, has assessed with high confidence that threats to the supply chain from both nation-states and criminal elements constitute a high cyber threat.⁶ Similarly, the National Counterintelligence Executive assessed that

“foreign attempts to collect U.S. technological and economic information will continue at a high level and will represent a growing and persistent threat to US economic security.”⁷

Third, the U.S. government must pay particular attention to products produced by companies with ties to regimes that present the highest and most advanced espionage threats to the U.S., such as China. Recent cyber-attacks often emanate from China, and even though precise attribution is a perennial challenge, the volume, scale, and sophistication often indicate state involvement. As the U.S.-China Commission explained in its unclassified report on China’s capabilities to conduct cyber warfare and computer network exploitation (CNE), actors in China seeking sensitive economic and national security information through malicious cyber operations often face little chance of being detected by their targets.⁸

Finally, complicating this problem is the fact that Chinese telecommunications firms, such as Huawei and ZTE, are rapidly becoming dominant global players in the telecommunications market. In another industry, this development might not be particularly concerning. When those companies seek to control the market for sensitive equipment and infrastructure that could be used for spying and other malicious purposes, the lack of market diversity becomes a national concern for the United States and other countries.⁹ Of note, the United States is not the only country focusing on these concerns. Australia expressed similar concerns when it chose to ban Huawei from its national broadband infrastructure project.¹⁰ Great Britain has attempted to address the concerns by instituting an evaluation regime that limits Huawei’s access to the infrastructure and evaluates any Huawei equipment and software before they enter the infrastructure.¹¹

A. China has the means, opportunity, and motive to use telecommunications companies for malicious purposes.

Chinese intelligence collection efforts against the U.S. government are growing in “scale, intensity and sophistication.”¹² Chinese actors are also the world’s most active and persistent perpetrators of economic espionage.¹³ U.S. private sector firms and cyber-security specialists report an ongoing onslaught of sophisticated computer network intrusions that originate in China, and are almost certainly the work of, or have the backing of, the Chinese government.¹⁴ Further, Chinese intelligence services, as well as private companies and other entities, often recruit those with direct access to corporate networks to steal trade secrets and other sensitive proprietary data.¹⁵

These cyber and human-enabled espionage efforts often exhibit sophisticated technological capabilities, and these capabilities have the potential to translate into efforts to insert malicious hardware or software implants into Chinese-manufactured

telecommunications components and systems marketed to the United States. Opportunities to tamper with telecommunications components and systems are present throughout product development, and vertically integrated industry giants like Huawei and ZTE provide a wealth of opportunities for Chinese intelligence agencies to insert malicious hardware or software implants into critical telecommunications components and systems.¹⁶ China may seek cooperation from the leadership of a company like Huawei or ZTE for these reasons. Even if the company's leadership refused such a request, Chinese intelligence services need only recruit working-level technicians or managers in these companies. Further, it appears that under Chinese law, ZTE and Huawei would be obligated to cooperate with any request by the Chinese government to use their systems or access them for malicious purposes under the guise of state security.¹⁷

A sophisticated nation-state actor like China has the motivation to tamper with the global telecommunications supply chain, with the United States being a significant priority. The ability to deny service or disrupt global systems allows a foreign entity the opportunity to exert pressure or control over critical infrastructure on which the country is dependent. The capacity to maliciously modify or steal information from government and corporate entities provides China access to expensive and time-consuming research and development that advances China's economic place in the world. Access to U.S. telecommunications infrastructure also allows China to engage in undetected espionage against the United States government and private sector interests.¹⁸ China's military and intelligence services, recognizing the technological superiority of the U.S. military, are actively searching for asymmetrical advantages that could be exploited in any future conflict with the United States.¹⁹ Inserting malicious hardware or software implants into Chinese-manufactured telecommunications components and systems headed for U.S. customers could allow Beijing to shut down or degrade critical national security systems in a time of crisis or war. Malicious implants in the components of critical infrastructure, such as power grids or financial networks, would also be a tremendous weapon in China's arsenal.

Malicious Chinese hardware or software implants would also be a potent espionage tool for penetrating sensitive U.S. national security systems, as well as providing access to the closed American corporate networks that contain the sensitive trade secrets, advanced research and development data, and negotiating or litigation positions that China would find useful in obtaining an unfair diplomatic or commercial advantage over the United States.

In addition to supply chain risks associated with hardware and software, managed services also pose a threat. Managed services, sold as part of the systems maintenance

contract, allow for remote network access for everyday updates to software and patches to glitches. Unfortunately, such contracts may also allow the managed-service contractor to use its authorized access for malicious activity under the guise of legitimate assistance. Such access also offers an opportunity for more-tailored economic or state-sponsored espionage activities. Telecommunications companies such as Huawei are seeking to expand service portions of their business.²⁰

The U.S. Government has acknowledged these concerns with telecommunications supply chain risk for several years. Indeed, as one of twelve critical infrastructure protection priorities outlined in the White House's 2009 Comprehensive National Cybersecurity Initiative (CNCI), Supply Chain Risk Management (SCRM) is identified as a national concern. Similarly, the Executive Branch continues to review supply chain issues consistent with its National Strategy for Global Supply Chain Security, released in January 2012. A key part of the management of supply chain risk, as explained in the report, is to properly "understand and identify vulnerabilities to the supply chain that stem from both exploitation of the system by those seeking to introduce harmful products or materials and disruptions from intentional attacks, accidents, or natural disasters."²¹

B. Suggested "mitigation measures" cannot fully address the threat posed by Chinese telecommunications companies providing equipment and services to United States critical infrastructure.

Many countries struggle with the potential threats posed by untrustworthy telecommunications companies. In Great Britain, the government took initial steps (as part of an overall mitigation strategy) to address its concerns by entering into an agreement with Huawei to establish an independently managed Cyber Security Evaluation Centre (CSEC). CSEC conducts independent reviews of Huawei's equipment and software deployed to the United Kingdom's telecommunications infrastructure, and provides such results to the relevant UK carriers and UK government. The goal of the British government is to attempt to lessen the threat that Huawei products deployed in critical UK telecommunications infrastructure pose to the availability or integrity of UK networks.

Huawei and ZTE have proposed similar schemes for products entering the United States market, administered without U.S. government involvement, but by Electronic Warfare Associates or other private-sector security firms.²² These partnerships seek to address concerns that the companies could permit the Chinese government to insert features or vulnerabilities into their products, which would assist espionage or cyber warfare. Unfortunately, there are concerns that such efforts if taken in the United States

will fall short of addressing security concerns given the breadth and scale of the U.S. telecommunications market.

Post-production evaluation processes are a standard approach to determining the security properties of complex, software-intensive systems. Processes like the Common Criteria for Information Technology Security Evaluation and various private certification services define a process by which an evaluator measures a product against a set of standards and assigns a security rating. The rating is meant to help a consumer know how much confidence to place in the security features of the device or software package. Both the implementation of the system and the methodology used to develop it, as documented by the manufacturer, are typically used as evidence for the chosen rating. Further, such processes are not necessarily designed to uncover malicious code but to encourage a foundational security baseline in security-enabled products.

For a variety of technical and economic reasons, evaluation programs as proposed by Huawei and ZTE are less useful than one might expect. In fact, the programs may create a false sense of security that an incomplete, flawed, or misapplied evaluation would provide. An otherwise careful consumer may choose to forego a thorough threat, application, and environment-based risk assessment, and the costs such evaluations entail, because an accredited outside expert has “blessed” the product in some way.

One key issue not addressed by standardized third-party security evaluations is product and deployment diversity. The behavior of a device or system can vary wildly depending on how and where it is configured, installed, and maintained. For time and cost reasons, an evaluation usually targets a snapshot of one product model configured in a specific and often unrealistically restrictive way. The pace of technology development today drives products to evolve far more rapidly than any third-party comprehensive evaluation process can follow. The narrow configuration specification used during testing almost ensures that an evaluated device will be deployed in a way not specifically covered by a formal evaluation. A security evaluation of a complex device is useless if the device is not deployed precisely in the same configuration as it was tested.

The evaluation of products prior to deployment only addresses the product portion of the lifecycle of networks. It is also important to recognize that how a network operator oversees its patch management, its trouble-shooting and maintenance, upgrades, and managed-service elements, as well as the vendors it chooses for such services, will affect the ongoing security of the network.

Vendors financing their own security evaluations create conflicts of interest that lead to skepticism about the independence and rigor of the result. A product

manufacturer will naturally pursue its own interests and ends which are not necessarily aligned with all interests of the consumers. A different, but related, race to the bottom has been noted for the similarly vendor-financed Common Criteria evaluations.²³ The designers of the Common Criteria system understood this danger and implemented government certification for evaluators. The precaution seems mostly cosmetic as no certification has ever been challenged or revoked despite gaming and poor evaluation performance. Given similar concerns and about conflicts of interest, Huawei's U.K. evaluators of Huawei equipment have been vetted by the U.K. government and hold government security clearances, and the U.K. process has the support of the U.K. Carriers. It is not clear yet, however, that such steps would readily transfer to the U.S. market or successfully overcome the natural incentives of the situation and lead to truly independent investigations.

The task of finding and eliminating every significant vulnerability from a complex product is monumental. If we also consider flaws intentionally inserted by a determined and clever insider, the task becomes virtually impossible.²⁴ While there is a large body of literature describing techniques for finding latent vulnerabilities in hardware and software systems, no such technique claims the ability to find all such vulnerabilities in a pre-existing system. Techniques do exist that can prove a system implementation matches a design which has been formally verified to be free of certain types of flaws.²⁵ However, such formal techniques must be incorporated throughout the design and development process to be effective. They cannot currently be applied to a finished product of significant size or complexity. Even when embedded into a design and development process, formal techniques of this type do not yet scale to the size of complete commercial telecommunication systems. It is highly unlikely that a security evaluation partnership such as that proposed by Huawei or ZTE, independent of its competence and motives, will be able to identify all relevant flaws in products the size and complexity of core network infrastructure devices. If significant flaws remain in widely fielded products and processes that are known to a potential adversary, it seems like the evaluation process has provided only marginal benefit.

A security evaluation of potentially suspect equipment being deployed in critical infrastructure roles may seem like an answer to the security problems posed. Unfortunately, given the complexity of the telecommunications grid, the limitations of current security evaluation techniques, and the economics of vendor-financed analyses provide a sense of security but not actual security. Significant security is available only through a thoughtful design and engineering process that addresses a complete system-of-systems across its full lifecycle, from design to retirement and includes aspects such as discrete technology components, their interactions, the human environment, and threats

from the full spectrum of adversaries. The result of such a process should be a convincing set of diverse evidence that a system is worthy of our trust.²⁶

II. Investigation

A. Scope of Investigation

The House Permanent Select Committee on Intelligence is responsible for authorizing the intelligence activities of the United States and overseeing those activities to ensure that they are legal, effective, and properly resourced to protect the national security interests of the United States. Specifically, the Committee is charged with reviewing and studying on a continuing basis the authorities, programs, and activities of the Intelligence Community and with reviewing and studying on an exclusive basis the sources and methods of the community.²⁷ Along with this responsibility is the obligation to study and understand the range of foreign threats faced by the United States, including those directed against our nation's critical infrastructure. Similarly, the Committee must evaluate the threats from foreign intelligence operations and ensure that the country's counterintelligence agencies are appropriately focused on and resourced to defeat those operations.²⁸

The Committee's goals in this investigation were to inquire into the potential security risk posed by the top two Chinese telecommunications companies and review whether our government is properly positioned to understand and respond to that threat. An additional aim of this process has been to determine what information could be provided in an unclassified form to shed light on the key questions of whether the existence of these firms in our market would pose a national-security risk through the potential loss of control of U.S. critical infrastructure.

Of course, the United States' telecommunications sector increasingly relies on a global supply chain for the production and delivery of equipment and services. That reliance presents significant risks that other individuals or entities – including those backed by foreign governments – can and will exploit and undermine the reliability of the networks. Better understanding the supply-chain risks we face is vital if we are to protect the security and functionality of our networks and if we are to guard against national security and economic threats to those networks. The investigation's scope reflects the underlying need for the U.S. to manage the global supply chain system using a risk-based approach.

Recent studies highlight that actors in China are the source of more cyber-attacks than in any other country. The National Counterintelligence Executive, for example,

explained, in an open report on cyber-espionage, that “Chinese actors are the world’s most active and persistent perpetrators of economic espionage.”²⁹ Thus, the Committee focused on those companies with the strongest potential Chinese ties and those that also seek greater entry into the United States market. Both Huawei and ZTE are indigenous Chinese firms, with histories that include connections to the Chinese government. Both Huawei and ZTE have already incorporated United States’ subsidiaries, and both are seeking to expand their footprint in the United States market. Huawei has received, thus far, the greatest attention from analysts and the media. Given the similarities of the two companies, however, including their potential ties to the Chinese government, support by the Chinese government, and goals to further their U.S. presence, the Committee focused on both Huawei and ZTE.

Both Huawei and ZTE assert that the Committee should not focus only on them to the exclusion of all other companies that manufacture parts or equipment in China. The Committee recognizes that many non-Chinese companies, including U.S. technology companies, manufacture some of their products in China. But it is not only the location of manufacturing that is important to the risk calculation. It is also ownership, history, and the products being marketed. These may not be the only two companies presenting this risk, but they are the two largest Chinese-founded, Chinese-owned telecommunications companies seeking to market critical network equipment to the United States. To review supply chain risk, the Committee decided to focus first on the largest perceived vulnerabilities, with an expectation that the conclusion of this investigation would inform how to view the potential threat to the supply chain from other companies or manufacturers operating in China and other countries.

B. Investigative Process

The Committee’s investigative process included extensive interviews with company and government officials, numerous document requests, and an open hearing with a senior official from both Huawei and ZTE. Committee staff reviewed available information on the specific companies, and Committee staff and members met with Huawei and ZTE officials for lengthy, in-depth meetings and interviews. Committee staff also toured the companies’ facilities and factories.

Specifically, on February 23, 2012, Committee staff met with and interviewed corporate executives of Huawei at its corporate headquarters in Shenzhen, China. The delegation toured Huawei’s corporate headquarters, reviewed company product lines, and toured a large manufacturing factory. Officials involved in the discussion from Huawei included Ken Hu, Huawei’s Deputy Chairman of the Board and Acting CEO; Evan Bai,

Vice President of the Treasury Management Office; Charlie Chen, Senior Vice President in charge of Huawei (USA); Jiang Xisheng, Secretary of the Board; John Suffolk, Global Security Officer; and Rose Hao, Export Regulator.

On April 12, 2012, Committee staff met with and interviewed corporate executives of ZTE at its corporate headquarters in Shenzhen, China. In addition to these meetings, the delegation took a brief tour of ZTE's corporate headquarters, including a factory site. Officials from ZTE included Zhu Jinyun, ZTE's Senior Vice President, U.S. and North America Market; Fan Qingfeng, Executive Vice President of Global Marketing and Sales; Guo Jianjun, Legal Director; Timothy Steinert, Independent Director of the Board (and Ali Baba Counsel); Ma Xuexing, Legal Director; Cao Wei, Security and Investor Relations with the Information Disclosure Office; Qian Yu, Security and Investor Relations with the Information Disclosure Office; and John Merrigan, attorney with DLA Piper.

In May of 2012, Ranking Member Ruppersberger along with Committee members Representative Nunes, Representative Bachmann, and Representative Schiff traveled to Hong Kong to meet with senior officials of both Huawei and ZTE. In addition to the senior officials present at the staff meetings, the Committee members met with Ren Zhengfei, the founder and President of Huawei.

After the meetings, the Committee followed-up with several pages of written questions and document requests to fill in information gaps, inconsistent or incomplete answers, and the need for corroborating documentary evidence of many of the companies' factual and historical assertions. Unfortunately, neither company was completely or fully responsive to the Committee's document requests. Indeed, neither Huawei nor ZTE provided internal documents in response to the Committee's letter.³⁰ To attempt, again, to answer the remaining questions, the Committee called each company to an open hearing.

On September 13, 2012, the Committee held an open hearing with representatives of both ZTE and Huawei. The witnesses included Mr. Charles Ding, corporate senior vice president and Huawei's representative to the United States, and Mr. Zhu Jinyun, ZTE senior vice president for North America and Europe. The hearing was designed to be both thorough and fair. The witnesses were each given twenty minutes for an opening statement and each was aided by an interpreter during the question and answer portion of the hearing to ensure that the witnesses were given the maximum opportunity to understand the questions and answer completely and factually.³¹

Once again, the witnesses' answers were often vague and incomplete. For example, they claimed to have no understanding or knowledge of commonly used terms, could not answer questions about the composition of their internal Party Committees, refused to provide straightforward answers about their operations in the United States, sought to avoid answering questions about their histories of intellectual property protection, and claimed to have no understanding or knowledge of Chinese laws that force them to comply with the Chinese government's requests for access to their equipment. The companies' responses to the Committee's questions for the record after the hearing included similar evasive answers.

C. Investigative Challenges

This unclassified report discloses the unclassified information the Committee received when trying to understand the nature of these companies, the formal role of the Chinese government or Chinese Communist Party within them, and their current operations in the United States. In pursuing this goal, the Committee faced many challenges, some of which are shared by many who seek to understand the relationship between the government and business in China and the threat posed to our infrastructure. These challenges include: the lack of transparency in Chinese corporate and bureaucratic structures that leads to a lack of trust; general private sector concerns with providing proprietary or confidential information; fears of retribution if private-sector companies or individuals discuss their concerns; and uncertain attribution of cyber attacks.

The classified annex provides significantly more information adding to the Committee's concerns. That information cannot be shared publicly without risking U.S. national security. The unclassified report itself, however, highlights that Huawei and ZTE have failed to assuage the Committee's significant security concerns presented by their continued expansion into the United States. Indeed, given the companies' repeated failure to answer key questions thoroughly and clearly, or support those answers with credible internal evidence, the national-security concerns about their operations have not been ameliorated. In fact, given their obstructionist behavior, the Committee believes addressing these concerns have become an imperative for the country.

In addition to the Committee's discussions with the companies, the Committee investigators spoke with industry experts and former and present employees about the companies. Companies around the United States have experienced odd or alerting incidents using Huawei or ZTE equipment. Officials with these companies, however, often expressed concern that publicly acknowledging these incidents would be detrimental to their internal investigations and attribution efforts, undermine their ongoing efforts to defend their systems, and also put at risk their ongoing contracts.

Similarly, statements by former or current employees describing flaws in the Huawei or ZTE equipment and other potentially unethical or illegal behavior by Huawei officials were hindered by employees' fears of retribution or retaliation.³²

Further, the inherent difficulty in attributing the precise individual or entity responsible for known attacks within the United States continues to hinder the technological capability for investigators to determine the source of attacks or any connections among industry, government, and the hacker community within China.³³

III. Summary of Findings

Chinese telecommunications companies provide an opportunity for the Chinese government to tamper with the United States telecommunications supply chain. That said, understanding the level and means of state influence and control of economic entities in China remains difficult. As Chinese analysts explain, state control or influence of purportedly private-sector entities in China is neither clear nor disclosed.³⁴ The Chinese government and the Chinese Communist Party, experts explain, can exert influence over the corporate boards and management of private sector companies, either formally through personnel choices, or in more subtle ways.³⁵ As ZTE's submission to the Committee states, "the degree of possible government influence must vary across a spectrum."³⁶

The Committee thus focused primarily on reviewing Huawei's and ZTE's ties to the Chinese state, including support by the Chinese government and state-owned banks, their connections to the Chinese Communist Party, and their work done on behalf of the Chinese military and intelligence services. The Committee also probed the companies' compliance with U.S. laws, such as those protecting intellectual property, to determine whether the companies can be trusted as good corporate actors. The Committee did not attempt a review of all technological vulnerabilities of particular ZTE and Huawei products or components. Of course, the Committee took seriously recent allegations of backdoors, or other unexpected elements in either company's products, as reported previously and during the course of the investigation. But the expertise of the Committee does not lend itself to comprehensive reviews of particular pieces of equipment.

The investigation sought to answer several key questions about the companies that would, including:

- What are the companies' histories and management structures, including any initial ties to the Chinese government, military, or Communist party?

- How and to what extent does the Chinese government or the Chinese Communist Party exert control or influence over the decisions, operations, and strategy of Huawei and ZTE?
- Are Huawei and ZTE treated as national champions or otherwise given unfair or special advantages or financial incentives by the Chinese government?
- What is the presence of each company in the United States market and how much influence does the parent company in Shenzhen influence its operations in the United States?
- Do the companies comply with legal obligations, including those protecting intellectual property rights and international sanctions regimes (such as those with respect to Iran)?

The Committee found the companies' responses to these lines of inquiry inadequate and unclear. Moreover, despite repeated requests, the companies' consistently provided very little – if any – internal documentation substantiating their answers. The few documents provided could rarely be authenticated or validated because of the companies' failure to follow standard document-production standards as provided by the Committee and standard with such investigations. Moreover, the apparent control of the Chinese government over this information remains a hindrance to a thorough investigation. One of the companies asserted clearly both verbally and in writing that it could not provide internal documentation that was not first approved by the Chinese government.³⁷ The fact that Chinese companies believe that their internal documentation or information remains a "state secret," only heightens concerns about Chinese government control over these firms and their operations.

The Committee is disappointed that Huawei and ZTE neither answered fully nor chose to provide supporting documentation for their claims, especially given that Huawei requested a thorough and complete investigation. The Committee simply cannot rely on the statements of company officials that their equipment's presence in U.S. critical infrastructure does not present a threat, and that the companies are not, or would not be, under pressure by the Chinese government to act in ways contrary to United States interests. The findings below summarize what the Committee has learned from information available, and suggest avenues for further inquiry.

A. The Committee finds that Huawei did not fully cooperate with the investigation and was unwilling to explain its relationship with the Chinese government or Chinese Communist Party, while credible evidence exists that it fails to comply with U.S. laws.

Throughout this investigation, Huawei officials sought to portray the company as transparent. Huawei consistently refused, however, to provide detailed answers in

written form or provide internal documentation to support their answers to questions at the heart of the investigation. Specifically, Huawei would not fully describe the history, structure, and management of Huawei and its subsidiaries to the Committee's satisfaction. The Committee received almost no information on the role of Chinese Communist Party Committee within Huawei or specifics about how Huawei interacts in formal channels with the Chinese government. Huawei refused to provide details about its business operations in the United States, failed to disclose details of its dealings with the Chinese military or intelligence services, and would not provide clear answers on the firm's decision-making processes. Huawei also failed to provide any internal documents in response to the Committee's written document requests, thus impeding the Committee's ability to evaluate fully the company's answers or claims.

In addition to discussions with Huawei officials, the Committee has interviewed several current and former employees of Huawei USA, whose employees describe a company that is managed almost completely by the Huawei parent company in China, thus undermining Huawei's claims that its United States operations are largely independent of parent company. The testimony and evidence of individuals who currently or formerly worked for Huawei in the United States or who have done business with Huawei also brought to light several very serious allegations of illegal behavior that require additional investigation. The Committee will refer these matters to the Executive Branch for potential investigation.

These allegations were not the focus or thrust of the investigation, but they were uncovered in the course of the investigation. The Committee believes that they reveal a potential pattern of unethical and illegal behavior by Huawei officials, allegations that of themselves create serious doubts about whether Huawei can be trusted to operate in the United States in accordance with United States legal requirements and international codes of business conduct.

- i. Huawei did not provide clear and complete information on its corporate structure and decision-making processes, and it likely remains dependent on the Chinese government for support.**

Huawei markets itself as a “leading global ICT [“Information Communications Technology”] solution provider,” that is “committed to providing reliable and secure networks.”³⁸ Throughout the investigation, Huawei consistently denied having any links to the Chinese government and maintains that it is a private, employee-owned company.³⁹ Many industry analysts, however, have suggested otherwise; many believe, for example, that the founder of Huawei, Ren Zhengfei, was a director of the People’s Liberation

Army (PLA) Information Engineering Academy, an organization that they believe is associated with 3PLA, China's signals intelligence division, and that his connections to the military continue.⁴⁰ Further, many analysts suggest that the Chinese government and military proclaim that Huawei is a "national champion" and provide Huawei market-distorting financial support.⁴¹

In seeking to understand the Chinese government's influence or control over Chinese telecommunications companies, the Committee focused on Huawei's corporate structure and decision-making processes. Better information about Huawei's corporate structure would also help answer lingering questions caused by Huawei's historic lack of transparency.⁴² For years, analysts have struggled to understand how Huawei's purported employee-ownership model works in practice, and how that ownership translates into corporate leadership and decision-making.⁴³ Huawei repeatedly asserts that it is a private, employee-owned and controlled company that is not influenced by the Chinese government or Chinese Communist Party.⁴⁴ Executives also asserted that the unique shareholder and compensation arrangement is the foundation of the company's rise and success.

Available information does not align with Huawei's description of this structure, and many analysts believe that Huawei is not actually controlled by its common shareholders, but actually controlled by an elite subset of its management.⁴⁵ The Committee thus requested further information on the structure of the company's ownership. For example, the Committee requested that Huawei list the ten largest shareholders of the company. Huawei refused to answer.⁴⁶ At the hearing on September 13, 2012, Huawei admits that its shareholder agreement gives veto power to Ren Zhengfei, the founder and president of the company.⁴⁷ Other public statements by the company undermine the suggestion that the 60,000 supposed shareholders of Huawei control the company's decisions. For example, in the company's 2011 report, Mr. Ren highlighted that Huawei's Board of Directors:

will not make maximizing the interests of stakeholders (including employees, governments, and suppliers) its goal. Rather, it holds on to the core corporate values that are centered on customer interests and encourage employee dedication.⁴⁸

Such statements undermine the credibility of Huawei's repeated claims that its employees control the company. Thus, to explore these conflicts, the Committee focused much attention on the shareholder program. Of note, the only nonpublic, purportedly internal documents that Huawei provided to the Committee in the course of the

investigation are unsigned copies of its shareholder agreement documents. Unfortunately, the Committee could not verify the legitimacy of these documents, because they were unsigned and non-official.

Huawei officials explained that Chinese law forbids foreigners from holding shares in Chinese companies absent a special waiver.⁴⁹ Current and former Huawei employees confirm that only Chinese nationals working at Huawei in the United States participate in the shareholding plan. The inability of non-Chinese employees of Huawei to hold shares of the company further erodes its claim that it is truly an employee-run organization as an entire group of employees are not only disadvantaged, but automatically excluded from any chance to participate in the process.

Huawei consistently asserted that the Chinese government has no influence over corporate behavior and that the company is instead managed as an employee-owned enterprise through Huawei's Employee Stock Ownership Program (ESOP). Officials explained that the shareholding plan is not a benefits plan; rather, it provides high-performing employees an option to buy dividend-providing shares and thereby share in the value of the company. Eligible employees are given the option to buy shares at a certain company determined price, and can only sell the shares when they leave the company or with approval.⁵⁰

Huawei also provided staff access to shareholder ballots for shareholder representatives and the Board of Directors. These too did not appear to be facially fraudulent, but they were impossible to authenticate, especially as investigators were not allowed to remove the documents from Huawei's facilities for third-party validation. The documents appeared to highlight that shareholders have a write-in option for union representatives, but there is no such option for the Board of Directors. Rather, Huawei officials stated that the nominees for the Board are chosen prior to the vote by the previous Board. It was unclear how the original Board was established, and Huawei has consistently failed to provide any answers about who was previously on its Board of Directors.

Huawei further explained that in 1994, the first Company Law of China was officially published, regulating the establishment and operations of limited liability companies.⁵¹ Under this law, the maximum number of shareholders was 50 individuals. Thus, in 1997, Huawei claims to have changed its legal structure to a limited liability company, and started the employee stock ownership program through the union. Similarly, Huawei asserted that in 1997, the City of Shenzhen issued policies regarding

employee shareholdings. According to Huawei, it designed its shareholder program to conform to the the Company Law of China, and the laws and policies of the City of Shenzhen.⁵²

According to Huawei, the union, known as Union of Huawei Investment and Holding Co., Ltd., facilitates ESOP implementation. The Union is a lawfully registered association of China. Huawei officials stated that “Huawei’s success can be directly linked to the company’s unique compensation structure.”⁵³ Currently, Huawei claims that the Union holds 98.7% of the ESOP shares, and Mr. Ren holds 1.3%. At the Huawei explained that as of December 31, 2011, ESOP has 65,596 participants, which it alleges are all Huawei employees (current and retired), it claims that there are no third parties, including government institutions, holding any ownership-stake in the company.

Questions remained after the Committee staff’s meeting with Huawei officials. Most importantly, the Committee did not receive clear information about how precisely candidates for the Board of Directors are chosen. This is a concern because such individuals are key decision-makers of the company and those whose potential connections to the government are of high concern. According to Huawei officials, the previous Board nominates the individuals for the current Board. But it is not clear how the original Board was established and Huawei refuses to describe how the first Board of Directors and first Supervisory Board were chosen.⁵⁴

As described above, Huawei provided the Committee unsigned, unauthenticated documents purporting to be: (1) Articles of Restricted Phantom Shares; (2) Letter of Undertakings of Restricted Phantom Shares; (3) Notice of Share Issuance and Confirmation Letter; (4) List of Shareholding Employees; (5) Record of Employee Payments and Buyback, (6) Receipts of Employee Share Payments and Buyback; (7) Election Records of the 2010 ESOP Representatives Election (procedures, ballots, results, announcements, etc.); (8) and conclusions of the 2010 ESOP Representatives Meeting. The Committee could not validate the legitimacy of these documents given that Huawei only provided unsigned drafts. Below are summaries of key information from these documents.⁵⁵

(1) ESOP Restricted Phantom Shares--Summary

- ESOP Restricted Phantom Shares Article 20 states that target grantees of employee stocks are current employees with high performance.

- Each year, the company determines the numbers of shares an employee can purchase based on job performance. Eligible employees must sign the Confirmation Letter and the Letter of Undertakings and make payments for the shares.
- An employee's stocks can be held only by the employee him/herself, and cannot be transferred or disposed by the employee. When an employee leaves the company (except for those who meet the retirement requirements with minimal eight years of tenure and 45 years old), stocks will be purchased back by the company.
- The current stock price is the net asset value of the stock from the previous year. When an employee purchases more shares or the Union takes shares back, it is based on the current stock price. The dividend amount of each year is based on the performance of the company.

(2) Articles of Restricted Phantom Shares—

a. The Commission

- The Commission is composed of 51 Representatives and nine alternates, elected by the Active Beneficiaries as organized by the Union with a term of five years.
 - Active beneficiary is defined as an active employee who works at Shenzhen Huawei Investment and Holding Co, Ltd or any of its equity affiliates and participates in the Plan of the Union.
 - In the event there is a vacancy, the Alternate shall take up the vacancy in sequence. The Alternates can attend, but not vote at, all meetings.
 - The Commission reviews and approves restricted phantom share issuance proposals; reviews and approves dividend distribution proposals; reviews and approves reports of the

board of shareholding employees; elects and replaces any member of the board; elects and replaces any member of Supervisory Board; reviews and approves procedures for electing representatives; approves amendments of these articles; reviews and approves the use of the reserve fund; reviews and approves other material matters with respect to restricted phantom share; perform functions as the shareholders of the company, exercises the rights of the shareholder, and develops resolutions regarding material matters such as capital increase, profit distribution, and selection of Directors and Supervisors.

- Meetings of the Commission shall be convened at least once a year, and shall be convened by the Board and presided over by the Chairman of the Board or the Vice Chairman.

b. The Board

- The Board is responsible for regular management authority and shall be responsible to the Commission.
- The main functions of the Board are to: prepare restricted phantom share issuance proposal; preparation of the dividends distribution proposal; formulation, approval, and amendment of the detailed rules, processes, and implementation methods with respect to the restricted phantom shares; preparation of the amendments to articles; determination on the detailed proposal as to the use of the Reserve Fund; execution of the resolutions of the Commission; exercise of the specific rights and powers of a shareholder of the Investee Company except for the matters on which a resolution from Commission is required; determination of other matters that shall be determined by the Board.
- The Board consists of 13 directors selected by the Commission; each serves for five years.

- The Board must convene at least once a year; it needs 2/3 present, and resolutions of the meetings shall be approved by at least 1/2 of all Directors.
- The Board may establish a restricted phantom share management committee and other necessary organizations responsible for carrying out and implementing the work assigned by the Board and for detailed matters with respect to the management of the restricted phantom shares, such as evaluation, distribution, and repurchase of the restricted phantom shares as well as management of the account and the Reserve Fund/treasury shares related to restricted phantom shares.

c. Supervisory Board

- The Supervisory Board is the organization responsible for supervising the implementation of the shareholder plan with its main functions and powers as follows:
 - supervising the implementation of the resolutions by the Board;
 - making recommendations or inquiries in event of any violation of any law, regulation or these Articles by the Board;
 - making work reports to the Commission; and
 - other regular functions and powers.
- Supervisors may attend Board meetings as non-voting delegate.
- The Supervisory Board shall consist of five Supervisors who shall be elected by the Commission to five year terms; no Director can serve concurrently as a Supervisor.
- Convene at least once a year, need minimum of 2/3 present, resolutions require approval of at least 2/3 of all Supervisors

d. Validity of Resolutions

- Before 31 December 2018, Mr. Ren shall have a right to veto the decisions regarding restricted phantom shares and Huawei's material matters (resolutions of the Board, Commission, and Shareholder's Meeting of the Company).
- Starting from 1 January 2013, the confirmed Active Beneficiaries who represent a minimum of 15% of the restricted phantom shares (excluding the restricted phantom shares held by the Restructuring Beneficiaries and the Retained Restricted Phantom Shares) shall have a right to veto the decisions regarding restricted phantom shares and Huawei's material matters (including resolutions of the Board, the Commission, and the Shareholders' Meeting of the Company).
- The relevant resolutions shall take effect in the event that the owner(s) of the right of veto does (do) not exercise the right of veto against the aforementioned resolutions.

(3) Acquisition of Restricted Phantom Shares

- The restricted phantom shares of the Union shall be issued to those key employees of the Company who have displayed excellent work performance.
- The Restricted Phantom Share Management Committee shall decide annually whether to issue shares, and the number of shares to be issued, based on the comprehensive evaluation of the work performance of such employee and in accordance with the evaluation rules of the restricted phantom shares. Retired or restructuring beneficiaries are not allowed to purchase new shares.

(4) Confidentiality and Non-Competition Obligations of the Beneficiaries

- No Active Beneficiary or Restructuring Beneficiary shall directly or indirectly have a second job in any way, work for any enterprise other than the Company without written consent of the Company or without entering into the relevant agreement with the Company.

ii. Huawei failed to explain its relationships with the Chinese government, and its assertions denying support by the Chinese government are not credible.

The nature of the modern Chinese economy is relevant for understanding Huawei’s connection to the Chinese state. The Chinese government often provides financial backing to industries and companies of strategic importance. Indeed, analysts of the Chinese political economy state that:

Huawei operates in what Beijing explicitly refers to as one of seven “strategic sectors.” Strategic sectors are those considered as core to the national and security interests of the state. In these sectors, the CCP [Chinese Communist Party] ensures that “national champions” dominate through a combination of market protectionism, cheap loans, tax and subsidy programs, and diplomatic support in the case of offshore markets. Indeed, it is not possible to thrive in one of China’s strategic sectors without regime largesse and approval.⁵⁶

Similarly, the U.S.-China Commission has explained, with Chinese companies, “the government’s role is not always straightforward or disclosed.” Despite some reforms, “much of the Chinese economy remains under the ownership or control of various parts of the Chinese government.”⁵⁷ The U.S. China-Commission lists Huawei as a form of enterprise in China that exists in a relatively new market and receives generous government policies to support its development and impose difficulties for foreign competition.⁵⁸

The Committee thus inquired into the precise relationship between the Chinese government and Huawei. During the Committee’s meetings with Huawei executives, and during the open hearing on September 13, 2012, Huawei officials consistently denied having any connection to or influence by the Chinese government beyond that which is typical regulation.⁵⁹ Specifically, Huawei explained in its written responses to the Committee, that “Huawei maintains normal commercial communication and interaction with relevant government supervisory agencies, including the Ministry of Industry and Information Technology and the Ministry of Commerce.”⁶⁰ Huawei claims that it “does not interact with government agencies that are not relevant to its business activities, including the Ministry of National Defense, the Ministry of State Security, and the Central Military Commission.”⁶¹ Huawei, however, did not provide information with which the Committee could evaluate these claims, as Huawei refused to answer the

specific questions of the Committee inquiring about the company’s precise mechanisms of interaction with and regulation by these government bodies.

The Committee did not expect Huawei to prove that it has “no ties” to the government. Rather, in light of even experts’ lack of certainty about the state-run capitalist system in China, the Committee sought greater understanding of its actual relationship with the Chinese government. The Committee requested that Huawei support and prove its statements about its regulatory interaction by providing details and evidence explaining the nature of this formal interaction. Any company operating in the United States could very easily describe and produce evidence of the federal entities with which it must interact, including which government officials are their main points of contact at those regulatory agencies.

In its written submission in response to the Committee’s questions, Huawei simply asserted that it “maintains normal commercial communication and interaction with relevant government supervisory agencies, including the Ministry of Industry and Information Technology and the Ministry of Commerce.”⁶² Huawei’s failure to provide further detailed information explaining how it is formally regulated, controlled, or otherwise managed by the Chinese government undermines the company’s repeated assertions that it is not inappropriately influenced by the Chinese government. Huawei appears simply unwilling to provide greater details that would explain its relationships with the Chinese government in a way that would alleviate security concerns.

Similarly, Huawei officials did not provide detailed answers about the backgrounds of *previous* Board Members. Rather, the Committee simply received the same biographies as previously disclosed of current members of the Board of Directors and Supervisory Board.⁶³ Previous Board Members may have significant ties to the Party, military, or government. And since the previous Board is responsible for nominating the current Board members, this information is important to understanding the historical progression of the company. Because the biographies of the previous members would highlight possible connections to military or intelligence elements of the Chinese government, Huawei’s consistent failure to provide this information is alerting.

iii. Huawei admits that the Chinese Communist Party maintains a Party Committee within the company, but it failed to explain what that Committee does on behalf of the Party or which individuals compose the Committee.

Huawei’s connection to the Chinese Communist Party is a key concern for the Committee because it represents the opportunity for the State to exert its influence over

the decisions and operations of a company seeking to expand into the critical infrastructure in the United States. This concern is founded on the ubiquitous nature of the Chinese Party in the affairs of institutions and entities in China, and the consensus view that the Party exerts pressure on and directs the resources of economic actors in China.⁶⁴

In response to the numerous opportunities to answer questions about its connection to the Party, Huawei stated that the company has no relevant connections. For example, in response to the Committee's written questions about the role of the Party in the company's affairs, Huawei merely stated that it "has no relationship with the Chinese Communist Party in its *business activities.*"⁶⁵

Huawei admits, however, that an internal Party Committee exists within Huawei. Huawei simply states that party committees are required by Chinese law to exist in all companies in China.⁶⁶ The existence of these Committees is, however, of particular relevance. Huawei states in its defense that all economic institutions in China are required to have a state Party apparatus inside the company. This is not, however, a compelling defense for companies seeking to build critical infrastructure in the United States. Indeed, experts in Chinese political economy agree that it is through these Committees that the Party exerts influence, pressure, and monitoring of corporate activities. In essence, these Committees provide a shadow source of power and influence directing, even in subtle ways, the direction and movement of economic resources in China.⁶⁷ It is therefore suspicious that Huawei refuses to discuss or describe that Party Committee's membership. Huawei similarly refuses to explain what decisions of the company are reviewed by the Party Committee, and how individuals are chosen to serve on the Party Committee.

Similarly, Huawei officials did not provide information about Mr. Ren's role or stature in the Party. In his official biography, Mr. Ren admits that he was asked to be a member of the 12th National Congress of the Communist Party of China in 1982. The National Congress is the once-in-a-decade forum through which the next leaders of the Chinese state are chosen. The Party members asked to play a role in China's leadership transition are considered key players in the state apparatus.⁶⁸ Mr. Ren proudly admits that he was invited to that Congress, but he will not describe his duties. Shortly after being given such a prestigious role, Mr. Ren successfully founded Huawei, though he asserts he did so without any government or Party assistance.⁶⁹ Huawei likewise refuses to answer whether Mr. Ren has been invited to subsequent National Congresses or has played any role in Party functions since that time.⁷⁰

From the review of available information, Huawei may have connections and ties to Chinese leadership that it refuses to disclose. In light of Huawei's refusal to discuss details of its acknowledged Chinese Communist Party Committee, the Committee questions the company's ability to be candid about any other possible connections to the government, military, or Chinese Communist Party.

iv. Huawei's corporate history suggests ties to the Chinese military, and Huawei failed to provide detailed answers to questions about those connections.

Huawei explained the founding and development of the company by focusing on the life and history of Ren Zhengfei, Huawei's founder. According to Huawei officials, Mr. Ren was a member of the Chinese military's engineering corps as a soldier tasked to establish the Liao Yang Chemical Fiber Factory and was promoted as a Deputy Director, which was a professional role equivalent to a Deputy Regimental Chief, but without military rank.⁷¹ Mr. Ren then retired from the army in 1983 after the engineering corps disbanded, and next worked for a State Owned Enterprise (SOE) following his retirement. According to this account, Mr. Ren was "dissatisfied" with his low salary and career path at the SOE, so in 1987, he established Huawei. Huawei officials did not explain how he was able to leave his employment with a SOE or whether he got agreement of the state to do so. Huawei officials denied that Mr. Ren was a senior member of the military.⁷² The Committee's requests for more information about Mr. Ren's military and professional background were unanswered. Huawei refused to describe Mr. Ren's full military background. Huawei refused to state to whom he reported when he was in the military. Huawei refused to answer questions about how he was invited to join the 12th National Congress, what duties he performed for the Party, and whether he has been asked to similar state-party matters.

Huawei similarly denied allegations that Ms. Sun Yafang, Chairwoman of Huawei, was previously affiliated with the Ministry of State Security. Mr. Ding responded to Committee questions after the hearing that, to his knowledge, reports about Ms. Yafang in Chinese publications, such as those in *Xinjing Bao*, are erroneous.⁷³ Mr. Ding did not respond to questions asking about how such publications received such information, or whether Ms. Yafang's previous biography on the Huawei website was erroneous as well. Rather, Mr. Ding simply provided again Ms. Yafang's corporate biography from the Huawei Annual Report 2011.⁷⁴

With respect to Huawei's founders, Huawei cited a Chinese legal requirement that new companies in the economic development zone must have a minimum of five

shareholders and 20,000 RMB registered capital. During meetings with the Committee, Huawei officials claimed that in 1987, Mr. Ren raised 21,000 RMB with personal savings and five other private investors. To the best of the officials' knowledge, none of the five investors had worked with Mr. Ren prior to start-up and one individual has previous affiliation with the government.⁷⁵ According to Huawei officials, the five investors never actually worked for Huawei and withdrew their investments several years later.⁷⁶

The Committee struggled to get answers from Huawei on the details of this founding, including how Mr. Ren came to know the initial individual investors, whether his connections to the military were important to the eventual development of the firm, and whether his role in the Party remains a factor in his and his company's success.

v. The Committee finds that Huawei's failure to provide information about the Chinese government's 1999 investigation of the company for tax fraud exemplifies how it refuses to be transparent; the apparent ease with which Huawei ended the investigation undermines Huawei's assertion that the Chinese government finds Huawei to be a disfavored telecommunications solutions provider in China.

Huawei officials claimed that after growing in rural areas in China throughout the 1990s, the Chinese government investigated the company at length between 1998-99 for tax fraud.⁷⁷ Huawei officials stated that they believed this investigation was politically motivated and performed at the urging of the company's competition – specifically, other telecommunications companies that are also state-owned enterprises. Mr. Ken Hu explained the investigation was a turning point in the history of the company. Specifically, Mr. Hu stated that Huawei's movement to opportunities outside of China was the result of this investigation.⁷⁸ Indeed, these officials sought to explain that this episode proves that Huawei was not in fact a "national champion" or otherwise a favored company in China.⁷⁹

Given the obvious importance Huawei placed on this tax-fraud investigation, the Committee's subsequent questions and document requests sought detailed information and further documentary support for its version of events. In particular, the Committee sought information on the conclusion of the Chinese investigation. This information is particularly important to the Committee given the apparent pride displayed by certain Huawei officials in Shenzhen when describing how they successfully used their connections to end the investigation. The ability of these corporate officers to end a politically-motivated investigation suggests that Huawei officials were not as lacking in political power or influence with the government as they suggested.

Despite the importance placed on this event, Huawei failed to address the Committee's questions in its written submission.⁸⁰ The company also failed to provide any material that would support Huawei's assertions that the investigation was closed legitimately or without attendant conditions placed on Huawei.⁸¹

vi. Huawei failed to explain its relationships with western consulting firms, and any claims that its success is on account of those relationships, rather than support by the Chinese government, are not credible.

Huawei officials stated that one reason for the company's success was its reliance on the advice of western consulting firms, such as IBM, Accenture, and Price Waterhouse Cooper.⁸² Huawei sought to convince the Committee that it was the advice of these companies -- and not support by the Chinese government -- that explains Huawei's miraculous growth in recent years.⁸³

Because of the importance Huawei places on the advice given by these consulting firms, the Committee sought greater information and evidence showing that such advice had important effects for the company. The Committee made clear that it did not seek information on the terms of the contractual arrangements with the consulting firms, but rather what information they reviewed from Huawei and what advice was provided. The Committee offered to keep such information confidential to avoid concerns about disclosing proprietary information.

Huawei responded with only a vague description of the advice provided by these companies. Specifically, although “[s]ince 1997, Huawei has relied on western management consulting firms to help improve [its] capabilities, build [its] processes, and develop a comprehensive management system driven by customer requirements,” Huawei failed to provide details about how those companies reformed the company other than providing a few sentences mentioning standard business practices, including lead to cash (LTC), integrated product development (IPD), issue to resolution (ITR), and integrated financial services (IFS). Huawei, refused “to provide additional details as to [its] consultancy relationships” citing concerns about proprietary information contained in that advice.⁸⁴ The Committee explained that it is most interested in evidence revealing what Huawei did in response to the advice of these firms, and specifically financial or other evidence that supports its position that those changes were responsible for efficiencies, growth, and market success.⁸⁵ Huawei could have answered such questions without revealing proprietary information held by these companies.⁸⁶ The Committee

was also willing to enter into a confidentiality agreement with all parties, an offer Huawei declined to accept or pursue.⁸⁷

Huawei has made the details of this consulting advice relevant to this investigation by attributing its rapid success to the advice rendered by these consulting firms. It is not then reasonable for Huawei to withhold that information from the Committee so that it could evaluate those claims. If Huawei has within its possession information and documents that would prove that the advice given by these firms was key to Huawei's success, Huawei should provide such information.⁸⁸ The Committee was and remains willing to enter into confidentiality agreements with all parties to solve any concerns about the release of proprietary information. Huawei has failed to accept this offer. Its failure to do so is indicative of the lack of cooperation shown throughout this investigation.

vii. Huawei failed to answer key questions or provide supporting documentation for its claims to be financially independent of the Chinese government.

As a company of strategic importance to China, Huawei's stature will be reflected in the level of financial support and direction it receives from the Chinese government and Party.⁸⁹ One way to review that support and direction provided by the state is through the financing the company receives. Many industry experts and telecommunications companies describe below-market pricing.⁹⁰ Thus, the Committee sought more information about Huawei's financing, including its customer financing. Such financial information would also help provide greater understanding about the financial structuring of a firm that remains largely opaque.

During the Committee's hearing, Mr. Ding suggested he did not understand and had no knowledge of the term "national champion," which is often used to describe favored Chinese companies throughout the economic literature on China.⁹¹ The Committee finds that Mr. Ding's suggestion that he does not understand the term is not credible. Huawei itself provided Capitol Hill offices a slide presentation in November 2011, which used the term "national champion" several times.⁹² In response to the Committee's questions about use of the term in that document, Huawei did not deny that it used the document and provided the document containing the term.⁹³ Rather, Huawei stated that the particular slide in the larger document was created by a third party and thus not Huawei's responsibility.⁹⁴ The Committee finds that Huawei's knowing use of the document in its discussions with United States elected representatives is sufficient evidence to prove that Huawei does in fact have an understanding of the term. Mr.

Ding's consistent refusal to answer questions about which firms are considered national champions in the Chinese telecommunications sector was obstructionist. In fact, his response to the Committee's question that "Huawei has not paid attention to the meaning of 'national champion' before," is obviously untrue given the company's use of the term in its presentations previously.⁹⁵ Moreover, his answers suggest that he did not want to explain how it was that Huawei, the number one telecommunications provider in China, is not a company of strategic importance in China, as recognized by others around the world.

Huawei officials also deny that they have received any special financial incentives or support from the Chinese government.⁹⁶ Huawei claimed that the company simply takes advantage of general Chinese banking opportunities, but does not seek to influence or coordinate with banks such as the Chinese Development Bank and the Export-Import Bank, which are both state owned. In previous presentations, Huawei had suggested that it served as an "intermediary and bridge" between the state-backed financial institutions and Huawei customers.⁹⁷ Huawei refused, however, to provide more detail about precisely how those lines of credit developed. Huawei also refused to answer specifics about its formal relationships with the Chinese banks, opting to simply answer that it maintains "normal business relations" with the Export-Import Bank of China.⁹⁸

In its presentation to the Committee during the February meeting, Huawei provided a list of the Memoranda of Understanding (MOUs) it claims to have signed with Chinese banks for lines of credit for its customers.⁹⁹ Huawei admits that its customers have a US \$100 billion in credit available, yet Huawei asserts that only \$5.867 billion has been drawn in the period between 2005 and 2011. Further, in its written responses, Huawei states that it is a "financing opportunity available to customers, not to Huawei."¹⁰⁰ Yet Huawei explained at the February 23, 2012, meeting with Committee investigators that the goal of the large available credit lines was for China "to appear impressive" and that "Huawei had to participate or would no longer receive loans" from Chinese banks.¹⁰¹ In response to repeated questions and document requests, Huawei failed to provide further written explanation of the benefits Huawei gains from these financing arrangements, and it did not provide internal documents or any auditable information that would substantiate its claims about the scope and processes of this financing.

Similarly, Huawei refused to describe the details of its relationships with Chinese state-owned banks. For example, in Mr. Ding's statement for the record, he explained that Huawei receives loans from ten Chinese banks. But Mr. Ding refused to answer how many of those ten banking institutions in China are state-owned.¹⁰² As described in the

previous section, Huawei also refused to provide “additional details as to [its] consultancy relationships” because it would “include highly sensitive proprietary information” governed by non-disclosure agreements.¹⁰³ In response to Committee questions about Huawei’s success and whether it was owing to the company’s support from the Chinese government, Huawei represented to the Committee that its relationships with and advice received from these companies are the source of the company’s global success.¹⁰⁴ Because Huawei refuses to provide details on those relationships and advice rendered, the Committee cannot evaluate its claim that any of its success is due to these relationships. Accordingly, the Committee discounts the role played by these consulting companies, and continues to find it likely that Huawei has substantially benefited from the support of the Chinese government.

In sum, Huawei admits that its customers receive billions of dollars in support from Chinese state-owned banks and that it has received favorable loans from Chinese banks for years. Huawei refuses to provide answers to direct questions about how this support was secured, nor does it provide internal documentation or auditable financial records to evaluate its claims that the terms of these agreements comply with standard practice and international trade agreements. The Committee is equally concerned with statements by company leaders that undermine the Committee’s confidence in the financial information the company has provided. For example, in a June 2007 speech to Huawei employees in the United Kingdom, Mr. Ren stated that he appreciated the subsidiary’s attempt to create financial statements, “whether the data is accurate or not.”¹⁰⁵ Based on available information, the Committee finds that Huawei receives substantial support from the Chinese government and Chinese state-owned banks, which is at least partially responsible for its position in the global marketplace.

viii. Huawei failed to provide sufficient details or supporting documentation on its operations, financing, and management in the United States; evidence undermines its claims of being a completely independent subsidiary of Huawei’s parent company in Shenzhen, China.

To understand the United States’ current vulnerability to supply-chain threats posed by Huawei equipment, it is necessary to know the extent to which Huawei’s equipment is already placed in U.S. infrastructure. Because the U.S. telecommunications infrastructure is largely built and owned by the private sector, the U.S. government does not have the full picture of what is contained within it and thus is not yet fully informed to develop policies to protect that critical infrastructure from vulnerabilities.¹⁰⁶

The Committee thus asked Huawei for information on its contracts for products and services within the United States. Understanding the extent to which Huawei equipment already exists in the United States is necessary to evaluate the present risk to the country, as well as to confirm Huawei's statements about the size and scope of its operations in the United States. Unfortunately, Huawei failed to provide specific information about its dealings within the United States. Huawei did provide the Committee a list of Huawei's major customers in the United States: Cricket Communications; Clearwire; Cox TMI Wireless, Hibernia Atlantic, Level 3/BTW Equipment, Suddenlink; Comcast and Bend Broadband. Huawei, however, did not provide information on the size and scope of its operations, which elements of the infrastructure it is providing, and where these operations are located.¹⁰⁷

The information requested by the Committee about Huawei's contracts in the United States is also necessary to evaluate Huawei's claims that they comply with all laws and trade obligations regarding the price of their products and services.¹⁰⁸ To date, Huawei has failed to provide any information to validate its claims that the prices of Huawei's products are based on market conditions. Huawei's refusal to answer clearly or provide documents supporting its claims necessitates the Committee finding that Huawei's defense is not credible. The Committee considers it possible that Huawei receives substantial support from the Chinese government such that Huawei can market at least some of its products in the United States below the costs of production.

Similarly, the extent to which Huawei's subsidiaries in the United States operate independently of the parent company in Shenzhen remains unclear. Such information is important, because any connections between the parent company in China to the Chinese government might affect the operations and behavior of the company in the United States. The Committee therefore requested information on the extent to which Huawei USA's decisions are controlled, influenced, or reviewed by the parent company.

Huawei explained that the first US-based Huawei subsidiary was established in the United States in 2005 with headquarters in Plano, Texas. Huawei stated that the parent company does not require approval for individual contracts in the United States.¹⁰⁹ Rather, it stated that the Board of Directors in China does set general terms for operations in the United States, and the parent company can help mobilize resources and set strategy should the subsidiary need it. The Committee has heard from several former Huawei employees in the United States who dispute Huawei's explanation of its business model. Sources from around the United States have provided numerous specific instances of business decisions in the United States requiring approval by the parent company in China. In one instance, an individual with first-hand knowledge explained that senior

level executives in the United States could not sign a contract for cyber-security services in the United States without approval in China. In fact, in one instance, a contract previously signed by a U.S.-based senior official at Huawei was repudiated by the parent company.¹¹⁰ These employees provided documentary evidence, including internal memoranda and emails, discussing corporate policy from China. This description of Huawei's US subsidiaries also comports with reports about the ties between other Huawei subsidiaries and the parent company in China.¹¹¹

To resolve this conflict, the Committee sought more information through its written questions to understand the precise mechanisms through which the Huawei parent company in Shenzhen controls Huawei's strategy for entry and growth into the United States market. Concerns that Beijing's support to Huawei could impact the U.S. market were heightened by Huawei officials' statements to Committee staff that Huawei USA is given general guidance and "resources" from the parent company if needed.¹¹² In its written response, however, Huawei failed to answer the Committee's detailed questions or provide any further information about the level of coordination between Huawei USA and the parent company.¹¹³

The information and material provided by Huawei employees with first-hand access coupled with Huawei's failure to provide detailed, internal information, undermines Huawei's claims. For these reasons, the Committee does not find credible Huawei's claims that its U.S. subsidiaries operate independently of the Huawei headquarters in Shenzhen, China.

ix. Evidence shows that Huawei exhibits a pattern of disregard for the intellectual property rights of other entities and companies in the United States.

Huawei's ability to protect intellectual property rights is an important indicator of the company's ability to abide by the laws of the United States. Thus, the Committee sought greater information on Huawei's history of IP protection.

The Committee has reason to believe that Huawei is careless with its compliance with intellectual property protections. Investigators heard from numerous sources that Huawei has a checkered history when it comes to protecting the intellectual property of other entities.¹¹⁴ Specifically, several former employees of Huawei said it is known to purposely use the patented material of other firms. First-hand accounts of former employees suggest that Huawei does not appropriately purchase software applications for use by its employees.¹¹⁵ Similarly, the Committee heard from industry experts that

Huawei has purposely used and marketed patented products of other companies.¹¹⁶ Finally, the Committee is in receipt of a Huawei slide presentation that was provided to Capitol Hill offices that itself violates copyright obligations by knowingly using proprietary material from an outside, nonaffiliated consulting firm.¹¹⁷

Huawei officials consistently denied ever infringing other companies' intellectual property rights. Even with respect to the litigation with Cisco, in which Huawei agreed to remove certain products from the marketplace, Huawei asserts that it had not violated Cisco's interests.¹¹⁸ Rather, Huawei suggested that the expert's review in that case of their equipment found no infringement of Cisco patents.¹¹⁹

Huawei's defense is not credible. First, with respect to the Cisco litigation, Huawei's statements do not comport with statements made by Huawei officials at the time of the lawsuit acknowledging that the company will remove infringing equipment.¹²⁰ Second, the Cisco settlement itself required Huawei to "update and change all of the products that have been accused of violating copyright or intellectual property rights."¹²¹ Finally, during the hearing on September 13, 2012, Charles Ding refused to answer the clear question of whether Cisco code had ever been in Huawei equipment.¹²² Mr. Ding's obstructionism during the hearing undermines Huawei's claims that it did not violate Cisco's patented material.

The Committee finds that Huawei's denials of intellectual property infringement were not credible or supported by available evidence. Because Huawei failed to produce any internal documents or support for its defenses, the Committee finds that Huawei has exhibited a pattern of, at the very least, reckless disregard for the intellectual property rights of other entities.

x. Huawei failed to provide details of its operations in Iran, though it denied doing business with the government of Iran, and did not provide evidence to support its claims that it complies with all international sanctions or U.S. export laws.

Huawei's ability to comply with international sanctions regimes and U.S. export control regulations is an important indicator of the company's ability to comply with international standards of corporate behavior and to abide by U.S. laws irrespective of China's influence or interests. Public reporting raises questions about the company's compliance with these laws.

In response to the Committee’s questions, Huawei officials provided only vague assertions about their commitment to all laws. Specifically, Huawei asserted that the company seeks to abide by all legal obligations and has transformed its business practices with the help of outside consultants to better monitor its actions to ensure compliance with international sanctions regimes. To highlight the lack of influence of the Chinese regime over its decisions, Huawei indicated the Chinese Embassy in Iran was surprised by Huawei’s decision to limit its business dealings in Iran. Huawei also stated that it does not allow its employees to participate in cyber activities, such as population monitoring, anywhere in Iran.

Huawei has refused, however, to answer detailed questions about its operations in Iran or other sanctioned countries. In its written submission to the Committee, Huawei again reiterated that it limited its future business in Iran because of the enhanced sanctions and an inability to collect payment for operations in Iran. Huawei highlights, though, that “Huawei respects the contracts signed with [its] customers” and thus will not end current contracts in Iran.¹²³ Huawei claims to “observe laws and regulations of the UN, the U.S., the E.U. and other countries and regions on sanctions.”¹²⁴ It also claims to have instituted an internal program on trade compliance representing best practices to manage these issues.¹²⁵ But Huawei refused to provide any internal documents relating to its decision to scale-back operations in Iran or otherwise ensure compliance with U.S. laws.

Such documents would have validated Huawei’s claims that the decision was based on legal compliance requirements and not influenced by any pressure by the Chinese government.

xi. Huawei refused to provide details on its R&D programs, and other documents undermine its claim that Huawei provides no R&D for the Chinese military or intelligence services.

To understand the extent to which Huawei performs R&D activity on behalf of the Chinese military or intelligence services, the Committee asked for information about its activities on behalf of the Chinese government or military. Specifically, the Committee requested information on the technologies, equipment, or capabilities that the funding or grants by the Chinese government was supporting. In its written submission to the Committee, Huawei failed to provide responsive answers to the Committee’s questions about the specifics of government-backed R&D activities.¹²⁶ Rather, Huawei simply asserted that it only bid on R&D projects open to the rest of the industry.¹²⁷

Huawei similarly claimed in its meetings with the Committee that it does not provide special services to the Chinese military or state security services.¹²⁸

In its answers to the Committee's questions after the hearing, Huawei again simply asserted that it "has never managed any of the PLA's networks" and "has never been financed by the Chinese government for R&D projects for military systems." Huawei did admit, however, that it develops "transport network products, data products, videoconferencing products, and all centers, and voice over IP (VoIP) products" for the Chinese military "accounting for .1% of Huawei's total sales."¹²⁹ Huawei also claimed, however, that it "develops, researches, and manufactures communications equipment for civilian purposes only."¹³⁰

The Committee also received internal Huawei documentation from former Huawei employees showing that Huawei provides special network services to an entity the employee believes to be an elite cyber-warfare unit within the PLA.¹³¹ The documents appear authentic and official Huawei material, and the former employee stated that he received the material as a Huawei employee.¹³² These documents suggest once again that Huawei officials may not have been forthcoming when describing the company's R&D or other activities on behalf of the PLA.

The Committee finds that Huawei's statements about its sales to the Chinese military are inherently contradictory. The Committee also finds that Huawei's failure to respond fully to questions about the details of its R&D activities, coupled with its admission that it provides products for the Chinese military and documents received from employees, undermine the credibility of its assertion that it does not perform R&D activities for the Chinese government or military.

xii. Former and current Huawei employees provided evidence of a pattern and practice of potentially illegal behavior by Huawei officials.

During the course of the investigation, several former and current Huawei employees came forward to provide statements and allegations about Huawei's activities in the United States. Given the sensitivities involved, and to protect these witnesses from retaliation or dismissal, the Committee has decided to keep the identities of these individuals confidential. The Committee has received multiple, credible reports from these individuals of several potential violations by Huawei officials. Those allegations include:

- Immigration violations;
- Bribery and corruption;
- Discriminatory behavior; and
- Copyright infringement.

Specifically, the Committee heard from numerous employees that Huawei employees visiting from China on tourist or conference visas are actually working full-time at Huawei facilities, in violation of U.S. immigration law. Similarly, Huawei employees provided credible evidence that individuals coming to the United States on particular visas, for example, for jobs requiring engineering expertise were not in fact employed by Huawei as engineers. These and other alleged violations of immigration law will be referred to the Department of Homeland Security for review and potential investigation.

Second, employees have alleged instances fraud and bribery when seeking contracts in the United States.¹³³ Those allegations will be referred to the Justice Department for further review and potential investigation.

Third, employees with whom the Committee spoke discussed allegations of widespread discriminatory behavior by Huawei officials. These individuals assert that it is very difficult if not impossible for any non-Chinese national to be promoted in Huawei offices in the United States. Further, these employees assert that non-Chinese nationals are often laid-off only to be replaced by individuals on short-term visas from China.¹³⁴ These allegations will be referred to the appropriate agencies in the Executive Branch to review and consider.

Finally, the Committee heard from former Huawei employees that may constitute a pattern and practice of Huawei using pirated software in its United States facilities. As previously described, the Committee received information with Huawei's logo that knowingly and admittedly violated another firm's copyrighted material.¹³⁵ The Committee thus finds that Huawei has exhibited a careless disregard for the copyrighted material of other entities. As there may indeed be credibility to these employee allegations, the Committee will also refer these claims to the Justice Department for investigation.

B. ZTE failed to answer key questions or provide supporting documentation supporting its assertions, arguing that answering the Committee's

requests about its internal corporate activities would leave the company criminally liable under China's state-secrets laws.

ZTE sought to appear cooperative and timely with its submissions to the Committee throughout the investigation. ZTE consistently refused, however, to provide specific answers to specific questions, nor did the company provide internal documentation that would substantiate its many claims. As with Huawei, the Committee focused its review of ZTE on the company's ties to the Chinese state, as well as the company's history, management, financing, R&D, and corporate structure. The Committee did not receive detailed answers on a number of topics described below. ZTE did not describe its formal interactions with the Chinese government. It did not provide financial information beyond that which is publicly available. It did not discuss the formal role of the ZTE Communist Party Committee and only recently provided any information on the individuals on the Committee. The Committee did not receive details on ZTE's operations and activities in Iran and other sanctioned countries. Finally, ZTE refused to provide detailed information on its operations and activities in the United States.

Importantly as well, ZTE argued at great length that it could not provide internal documentation or many answers to Committee questions given fear that the company would be in violation of China's state-secrets laws and thus subject ZTE officials to criminal prosecution in China.¹³⁶ In fact, ZTE refused even to provide the slides shown to the Committee staff during the meeting in April, 2012, for fear that they might be covered by state secrets. To the extent ZTE cannot provide detailed and supported answers to the Committee because China's laws treat such information important to the security of the Chinese regime, the Committee's core concern that ZTE's presence in the U.S. infrastructure represents a national-security concern is enhanced.

The Committee notes that ZTE's many written submissions were never numbered to align with the Committee's specific questions and document requests, as would be typical with formal legal processes. The Committee believes that, through this method, ZTE sought to avoid being candid and obvious about which questions it refused to answer. Moreover, ZTE's answers were often repetitive, lacking in documentary or other evidentiary support, or otherwise incomplete.

The Committee also notes that ZTE did not simply deny all national-security concerns arising from the global telecommunications supply chain. ZTE has advocated for a solution – one based on a trusted delivery model – in which approved “independent third-party assessors” transfer “hardware, software, firmware, and other structural elements in the equipment to the assessor.”¹³⁷ Such a model, as advocated by ZTE,

would include among other things, a “thorough review and analysis of software codes,” “vulnerability scans and penetration test,” “review of hardware design and audit of schematic system diagram,” “physical facility review and independent comprehensive audit of vendor’s manufacturing, warehousing, processing, and delivery operations,” “periodic assessments.”

ZTE suggests that a model, as previously proposed by Huawei and other companies, and similar in some respects to that introduced in United Kingdom, be implemented across the spectrum for telecommunications equipment providers. As discussed above, the Committee remains concerned that, although mitigation measures can be of some assistance, this model fails to appreciate the nature of telecommunications equipment.

i. ZTE did not alleviate Committee concerns about the control of Chinese state-owned enterprises in ZTE’s business decisions and operations.

As with Huawei, the Committee is concerned with the influence of the Chinese state in ZTE’s operations. Such access or influence would provide a ready means for the Chinese government to exploit the telecommunications infrastructure containing ZTE equipment for its own purposes. To evaluate the ties to the Chinese state, the Committee focused on the company’s history, structure, and management. Many commentators have noted that ZTE’s founding included significant investment and involvement by Chinese state-owned enterprises, and thus the Committee sought to unpack the current operations and ownership structure with the hope of understanding whether there are remaining ties to the Chinese state.

ZTE describes itself as a global provider of telecommunications equipment and network solutions across 140 countries. Founded in 1985, ZTE states that its 2011 revenue led the industry with a 24% increase to \$13.7 billion; its overseas operating revenue grew 30% to U.S. \$7.42 billion during the period, accounting for 54.2% of overall operating revenue.¹³⁸ ZTE markets itself by explaining that its systems and equipment have been used by top operators in markets around the world. Importantly, ZTE also highlighted in its 2011 Annual Report that China’s 12th five-year national plan has significantly contributed to ZTE’s recent domestic success.¹³⁹

During the interviews with ZTE officials in April and May 2012, ZTE officials stressed that ZTE is a publicly traded company, having been listed on the Shenzhen stock exchange in 1997, and the Hong Kong stock exchange in 2004. ZTE contends that it did not begin with government assistance, either with technology transfers or financial

assistance. Rather, ZTE stated that the Chinese government became a shareholder during the 1997 public offering. ZTE has also asserted that the state-owned-enterprise shareholders have no influence on strategic direction of the company.¹⁴⁰ ZTE officials often contrasted themselves with Huawei, though often did not mention Huawei by name. In particular, officials suggested that Huawei is ZTE's main competitor, but often stated that ZTE is more transparent since it is a publicly traded company.

These officials often relied on this public listing to claim that ZTE finances are transparent and comply with both Chinese and Hong Kong regulations regarding financial disclosures. The officials often simply referred to the fact that they have annual reports that detail information requested, such as amount and extent of government loans, subsidies, and credits. ZTE refused, however, to explain whether it would be willing to meet the reporting and transparency requirements of a western stock exchange such as the New York Stock Exchange.¹⁴¹ As with Huawei, when the Committee sought more detailed answers from ZTE on its interactions with key government agencies, ZTE refused to answer.

The history and structure of ZTE, as admitted by the company in its submissions to the Committee, reveal a company that has current and historical ties to the Chinese government and key military research institutes. In response to questioning, the ZTE officials first discounted and seemingly contradicted their own public statements, which suggest that ZTE formed originally from the Ministry of Aerospace, a government agency. In fact, exhibits displayed during the meeting in Shenzhen highlighted an early collaboration between ZTE and the government-run No. 691 Factory, and other state-owned enterprises. ZTE refused to provide the Committee copies of the slides presented during this meeting.

ZTE officials instead suggested that Mr. Hou Weigui founded ZTE in 1985 with five other “pioneer” engineers. Although they had all previously worked for state owned enterprises, ZTE officials insisted that the formation of ZTE did not arise from any relationship with the government. The company’s written submission to the Committee admits that the company had an early connection to No. 691 Factory, which was established by the Chinese government.¹⁴² As described by ZTE, No. 691 Factory is now known as Xi’an Microelectronics Company, and is a subsidiary of China Aerospace Electronics Technology Research Institute, a state-owned research institute. In its submission, ZTE admits that Xi’an Microelectronics owns 34% of Zhongxingxin, a shareholder of ZTE.¹⁴³ ZTE’s evolution from research entities with connections to the Chinese government and military highlight the nature of the information-technology (IT) sector in China. In fact, taking as true ZTE’s submission of its history and ownership,

ZTE's evolution confirms the suspicions of analysts who study the IT sector in China and describe it as a hybrid serving both commercial and military needs.¹⁴⁴

In 1997, ZTE was publicly listed for the first time on the Shenzhen stock exchange. ZTE executives claim that it was at this point that other state owned enterprises began investing in ZTE.

Currently, 30% of ZTE is owned by Zhongxinxin group and the remaining 70% is held by dispersed public shareholders. The Committee is particularly interested in whether the 30% ownership by Zhongxingxin constitutes a controlling interest or otherwise provides the state owned enterprises an opportunity to exert influence over the company. This question is particularly relevant because two state owned enterprises own 51% of Zhongxingxin. ZTE executives stressed that the public ownership of ZTE is increasing as Zhongxingxin sells its shares (for example, in 2004, Zhongxingxin owned 44% of ZTE, and now Zhongxingxin holds only 30%). In ZTE's July 3 submission to the Committee, ZTE states that "[v]ery few knowledgeable individuals in China would characterize ZTE as a state-owned entity (SOE) or a government-controlled company."¹⁴⁵ But the Committee specifically asked how it is that ZTE remains accountable to its shareholders and not influenced or controlled by its largest shareholder given this ownership structure. In its submission to the Committee, ZTE admits that a 30% share is the point at which Hong Kong and Chinese law considers the holder to be a "controlling shareholder."¹⁴⁶ ZTE simply stated that the company's fiduciary duty to the numerous shareholders means that the controlling shareholder does not in fact exert much actual control over the company.¹⁴⁷ ZTE does not explain in more detail how the Board members, five of whom are chosen by state-owned enterprises, and some of whom are acknowledged members of the Chinese Communist Party and members of ZTE's internal Communist Party Committee, would not exert any influence over the decisions of the company.

Zhongxingxin, ZTE's largest shareholder is owned in part by two state-owned enterprises, Xi'an Microelectronics and Aerospace Guangyu, both of which not only have ownership ties to the Chinese government, but also allegedly partake in sensitive technological research and development for the Chinese government and military. ZTE failed to address the Committee's questions seeking detailed information on the history and mission of these two companies. ZTE also failed to answer questions about these companies' relationship to key leaders within ZTE, specifically Mr. Weigu Hou, and ZTE's other major shareholder, Zhongzing WXT.

Because ZTE failed to answer key questions about its history and the connections to government institutions, the Committee cannot trust that it is free of state influence, particularly through its major shareholders and Board members.

ii. ZTE maintains a Chinese Party Committee within the company, and has not fully clarified how that Committee functions, who chooses its members, and what relationship it has with the larger Chinese Communist Party.

As with Huawei, ZTE's connection to the Chinese Communist Party is a key concern for the Committee. Such a connection offers the Party the opportunity to influence the decisions and operations of a company seeking to expand into the critical infrastructure in the United States. As described previously, the modern Chinese state-capitalistic economy is largely influenced if not controlled by the Party, in large part through the party committees that exist within individual firms.

During interviews with ZTE officials, ZTE refused to answer whether the executives or board members are members of the Chinese Communist Party. ZTE first downplayed the existence of the Party Committee within ZTE, and company representatives were unable to answer whether any members of the Board were also members of the state Party. Subsequently, in response to continued Committee questions, ZTE acknowledged that it does, in fact, contain an internal Committee Party, which ZTE suggests is required by the laws of China.¹⁴⁸ In response to the Committee's written questions, ZTE again refused, however, to provide information about the names and duties of the Party Committee members. At the September 13, 2012, hearing, Mr. Zhu attested under oath that ZTE would provide the names of those individuals on the Party Committee.¹⁴⁹

In response to questions posed at the September 13, 2012, hearing ZTE did provide the Committee a list of 19 individuals who serve on the Communist Party Committee within ZTE. At least two of those individuals appear to be on the ZTE Board of Directors. Other individuals are major shareholders in ZTE entities. ZTE has requested and the Committee has agreed to keep the names of these individuals out of the public domain. ZTE discounts the influence of that these individuals may have over the company. The company asked that the Committee not release the names of the individuals for fear that the company or the individuals might face retaliation by the Chinese government or Communist Party. The Committee has decided to keep the names of those members out of this public report, but the company's concern with the potential retaliatory measures it faces by the government for simply providing the

Committee the names of an internal ZTE body highlights why this Committee remains very concerned that the Chinese state is, or could be, responsible for the actions of the company. China clearly seeks to maintain deep ties into and secrecy about its role in economic actors in China. The control Chinese government maintains over the company's actions and level of transparency is of particular concern when that company seeks to build critical U.S. infrastructure.

ZTE also did not fully explain the function of the Party Committee. Instead, ZTE simply states that the Party Committee is controlled by company management. This assertion is contradicted by ZTE's own statement that ZTE executives and board members actually are members of the [Chinese Communist Party] and delimit its activities.”¹⁵⁰ To the extent these executives and Board Members have obligations to both the company's shareholders and the State through the Communist Party, there is an inherent conflict of interest in their duties, and this statement provides confirmation that the Party likely does in fact have influence and input into the business affairs of the company through these individuals.

The affidavit by the independent director, Timothy Steinert, seeks to allay any concerns of influence by the government or Party by stating that:

In my experience and to my knowledge, no member of ZTE's Board of Directors has raised for consideration an interest on behalf of the Chinese Government, the People's Liberation Army or the Chinese Communist Party.¹⁵¹

This statement does not resolve the Committee's concerns. First, there is a range of operational and strategic decisions made on a daily basis within companies that are not decided by or reviewed by the Board. Mr. Steinert's affidavit says nothing about the role of the Party Committee in those decisions prior to their reaching the Board, or for decisions that do not reach the Board at all. Second, the Party's influence through ZTE's Party Committee may not be facially obvious in the decision documents appearing for review to the Board. Since at least two members of the Board are also members of the Chinese State Party, it is impossible to know whether the votes of the Board are conducted without influence by the Chinese Communist Party. When considering ZTE's activities or voting on certain measures, those Board members need not cite the Party to be acting on the state's behalf or in pursuit of the state's interests. For these reasons, the Committee finds unpersuasive ZTE's claims that Mr. Steinert's affidavit “confirms that ZTE business decision making is not influence by the government or Party considerations”¹⁵²

ZTE recently suggested that the Party Committee “performs only ceremonial and social functions.” For six months, the Committee has asked ZTE about the role of the Party Committee, but only at the final hour, did it provide any response at all. Without further information and specifics about the role and influence of the Party Committee in the operations of the company, the Committee simply cannot allay the concerns about the internal party apparatus existing within a company seeking to build U.S. critical infrastructure.

iii. ZTE failed to disclose information about its activities in the United States.

ZTE discussed its extensive presence in 140 countries, but significantly downplayed any potential threats to the U.S., by suggesting that 95% of its U.S. sales are from handsets. ZTE officials highlighted that they have five R&D centers in the U.S. employing about 300 people. ZTE officials attempted to suggest that the company’s presence in rural infrastructure and networks was to assist the U.S. effort with its rural broadband plans. Committee staff questioned this logic, and ZTE officials admitted that ZTE’s role in these projects were not for charity or public service, as they had initially suggested, but to get a “foothold” in the country and learn the technology in the United States. ZTE officials even admitted that they are willing to provide this equipment to the U.S. below cost in order to learn the U.S. market. Specifically, during the Committee’s meeting with ZTE officials in Shenzhen, Mr. Zhu stated that the company was willing to lose money on projects in the United States to get a foothold in the United States and to understand the technology and standards in the United States.

ZTE’s description of its current U.S. activity is simply a picture at a particular point in time. The Committee could not confirm the extent of the company’s contracts or access to the United States market absent responses to the Committee’s document requests.¹⁵³ Despite numerous requests, ZTE has not provided detailed information on infrastructure projects in the United States.¹⁵⁴ ZTE also failed to answer follow-up questions that would explain whether ZTE purposely bids on projects below cost and how the company is able to sustain these losses. Further, at the HPSCI hearing on September 13, Mr. Zhu reversed his previous answers and refused to acknowledge that ZTE ever bids below cost for projects in the United States.¹⁵⁵

iv. ZTE failed to provide any answers or evidence about its compliance with intellectual property or U.S. export-control laws.

The protection of intellectual property and compliance with United States export control laws are a core concern for U.S. interests. The ability of a company to comply

with these laws provide a useful test of that company's ability to follow international codes of business conduct and remain free of undue state influence.

Representatives of the company consistently declined to comment on recent media reports that ZTE had sold export-controlled items to Iran.¹⁵⁶ At the hearing on September 13, 2012, ZTE acknowledged that it is performing an internal review to determine if the company destroyed any documents or other evidence related to its activities in Iran.¹⁵⁷ Mr. Zhu provided no information that could allow the Committee to evaluate the extent of those activities, their compliance with U.S. laws, or management's involvement in the potential destruction of documents and evidence. ZTE did not answer in specific written questions from the Committee asking why it sought to limit its Iranian business activities; whether ZTE will honor its current contracts in Iran; or whether those contracts include training or maintenance of surveillance equipment. Further, ZTE refused to answer questions about what products ZTE resold in Iran. ZTE also refused to provide any documents on its activities in Iran.

v. ZTE failed to provide clear answers to Committee questions about its R&D activities, particularly as they relate to any military or government projects.

Given ZTE's background, the Committee was interested in ZTE's R&D activities, and particularly its R&D activities with or on behalf of the Chinese military or security services. This information would help the Committee evaluate whether a company seeking to build critical infrastructure in the United States could also be working with the Chinese government on R&D projects with the purpose of finding or exploiting vulnerabilities in those systems.

ZTE's known connections to Chinese government-related research institutes are of particular interest. For example, ZTE acknowledges that one of its primary shareholders, Zhongxingxin, is owned in part by Xi'an Microelectronics, a subsidiary of China Aerospace Electronics Technology Research Institute, a state-owned research institute.¹⁵⁸ Another 17% of Zhongxingxin is held by Aerospace Guangyu, a subsidiary of a state-owned enterprise whose business includes production of, among other things, aerospace technology products.¹⁵⁹ ZTE failed to answer questions from the Committee seeking further details about the range of products these research institute have produced on the Chinese government so the committee could not evaluate whether those technologies were produced for military or intelligence purposes.¹⁶⁰

These ties to Chinese government research institutes and production companies, the Committee sought more information on the details of ZTE's R&D activities, and

particularly its potential work on behalf of the government, military, or security services. ZTE was proud to explain that it had established 18 state-of-the-art R&D centers throughout China, France, and India, and to employ over 30,000 research professionals. ZTE further claims that 10% of the company's annual revenue is invested in R&D. ZTE failed, however, to answer Committee questions about the technologies it may create or sell to the Chinese government and military. During the Committee's April 12, 2012 meeting with company officials, Mr. Steinert, the independent board member, stated that, ZTE's work on behalf of the Chinese telecommunications providers that happen to be state-owned enterprises does not suggest that ZTE does work on behalf of the military or intelligence services. When providing written answers ZTE refused to provide clear answers about the nature and extent of any work it does on behalf of the Chinese military or security services. Rather, ZTE states that "[t]he funding ZTE has received from government or consortia during the past several years is indistinguishable from similar funding available throughout the world in companies engaged in R&D through normal procurement processes."¹⁶¹

To the extent ZTE's R&D activities are simply in response to standard government procurement processes, the Committee does not understand why it refuses to answer direct questions about the details of those projects. For this reason, the Committee cannot allay concerns that ZTE is aligned with Chinese military and intelligence activities or research institutes.

Conclusion and Recommendations

The Committee launched this investigation to seek answers to some persistent questions about the Chinese telecommunications companies Huawei and ZTE and their ties to the Chinese government. Throughout the months-long investigation, both Huawei and ZTE sought to describe, in different terms, why neither company is a threat to U.S. national-security interests. Unfortunately, neither ZTE nor Huawei have cooperated fully with the investigation, and both companies have failed to provide documents or other evidence that would substantiate their claims or lend support for their narratives.

Huawei, in particular, provided evasive, nonresponsive, or incomplete answers to questions at the heart of the security issues posed. The failure of these companies to provide responsive answers about their relationships with and support by the Chinese government provides further doubt as to their ability to abide by international rules.

Recommendations

Based on this investigation, the Committee provides the following recommendations:

Recommendation 1: The United States should view with suspicion the continued penetration of the U.S. telecommunications market by Chinese telecommunications companies.

- The United States Intelligence Community (IC) must remain vigilant and focused on this threat. The IC should actively seek to keep cleared private sector actors as informed of the threat as possible.
- The Committee on Foreign Investment in the United States (CFIUS) must block acquisitions, takeovers, or mergers involving Huawei and ZTE given the threat to U.S. national security interests. Legislative proposals seeking to expand CFIUS to include purchasing agreements should receive thorough consideration by relevant Congressional committees.
- U.S. government systems, particularly sensitive systems, should not include Huawei or ZTE equipment, including in component parts. Similarly, government contractors – particularly those working on contracts for sensitive U.S. programs – should exclude ZTE or Huawei equipment in their systems.

Recommendation 2: Private-sector entities in the United States are strongly encouraged to consider the long-term security risks associated with doing business with either ZTE or Huawei for equipment or services. U.S. network providers and systems developers are strongly encouraged to seek other vendors for their projects. Based on available classified and unclassified information, Huawei and ZTE cannot be trusted to be free of foreign state influence and thus pose a security threat to the United States and to our systems.

Recommendation 3: Committees of jurisdiction within the U.S. Congress and enforcement agencies within the Executive Branch should investigate the unfair trade practices of the Chinese telecommunications sector, paying particular attention to China's continued financial support for key companies.

Recommendation 4: Chinese companies should quickly become more open and transparent, including listing on western stock exchange with advanced transparency requirements, offering more consistent review by independent third-party evaluators of their financial information and cyber-security processes, complying with U.S. legal standards of information and evidentiary production, and obeying all intellectual-property

laws and standards. Huawei, in particular, must become more transparent and responsive to U.S. legal obligations.

Recommendation 5: Committees of jurisdiction in the U.S. Congress should consider potential legislation to better address the risk posed by telecommunications companies with nation-state ties or otherwise not clearly trusted to build critical infrastructure. Such legislation could include increasing information sharing among private sector entities, and an expanded role for the CFIUS process to include purchasing agreements.

¹ Ken Hu, "Huawei Open Letter." <http://online.wsj.com/public/resources/documents/Huawei20110205.pdf> (accessed August 2, 2012).

² Huawei's letter was issued in February, 2011, when the Committee on Foreign Investment in the United States (CFIUS) issued a recommendation that Huawei voluntarily divest assets it received in a 2010 deal with 3Leaf, a United States company that developed advanced computer technologies. Shayndi Raice, "Panel Poised to Recommend Against Huawei Deal," *Wall Street Journal*, February, 11, 2011. <http://www.wsj.com/article/SB20001424052748704629004576136340771329706.html> (accessed August 2, 2012)

³ A classified annex to this report provides both classified information relevant to the discussion, as well as information about the resources and priorities of the IC.

⁴ Steven M. Rinaldi, James P. Peerenboom, and Terrence K. Kelly, "Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies," *IEEE Control Systems Magazine*, December 2001.

⁵ "The former National Counterintelligence Executive, Mr. Robert Bryant, recently noted that, 'Insider threats remain the top counterintelligence challenge to our community.' An insider threat arises when a person with authorized access to U.S. Government resources, to include personnel, facilities, information, equipment, networks, and systems, uses that access to harm the security of the United States. Malicious insiders can inflict incalculable damage. They enable the enemy to plant boots behind our lines and can compromise our nation's most important endeavors. Over the past century, the most damaging U.S. counterintelligence failures were perpetrated by a trusted insider with ulterior motives."

<http://www.ncix.gov/issues/ithreat/index.php>

⁶ FBI, *Intelligence Bulletin*, "Supply Chain Poisoning: A Threat to the Integrity of Trusted Software and Hardware," June 27, 2011: 1.

⁷ Office of National Counterintelligence Executive, *Report to Congress on Foreign Economic Collection and Industrial Espionage*, "Foreign Spies Stealing US Economic Secrets in Cyberspace."(October 2011, Washington, DC: 1.)

⁸ United States Congress, *2011 Annual Report of U.S.-China Economic and Security Review*. (2011, Washington DC: 59.)

⁹ National Institute of Standards and Technology, *Draft NISTIR 7622*, "Piloting Supply Chain Risk Management for Federal Information Systems," June 2010, 28.

¹⁰ Joint Press Conference, March, 29, 2012, Sydney, Australia. <http://www.pm.gov.au/press-office/transcript-joint-press-conference-sydney-1>.

¹¹ The Economist, "Huawei: The Company that Spooked the World," *Economist*, August, 4, 2012. <http://www.economist.com/node/21559929> (accessed September 30, 2012).

¹² United States Congress, *2011 Annual Report of U.S.-China Economic and Security Review*. (2011, Washington DC: 148.)

¹³ Office of National Counterintelligence Executive, *Report to Congress on Foreign Economic Collection and Industrial Espionage*, “Foreign Spies Stealing US Economic Secrets in Cyberspace.”(October 2011, Washington, DC: i.)

¹⁴ Ibid, 5; HPSCI staff interviews with cyber-security experts.

¹⁵ Ibid, 5.

¹⁶ Defense Science Board, *Report on Mission Impact of Foreign Influence on DoD Software*, September 2007: viii.

¹⁷ “Where State security requires, a State security organ may inspect the electronic communication instruments and appliances and other similar equipment and installations belonging to any organization or individual.” State-Security Law of the People’s Republic of China, Article 11.

¹⁸ Defense Science Board, *Report on Mission Impact of Foreign Influence on DoD Software*, September 2007: viii.

¹⁹ Northrop Grumman Corp, *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage*, prepared for U.S.-China Economic and Security Review Commission, March 7, 2012, 6-8.

²⁰ The Economist, “The Long March of the Invisible Mr. Ren,” *the Economist*, June 2, 2011.

<http://www.economist.com/node/18771640> (accessed on September 15, 2012).

²¹ FBI, *Intelligence Bulletin*, “Supply Chain Poisoning: A Threat to the Integrity of Trusted Software and Hardware,” June 27, 2011: 4.

²² ZTE, *Submissions to HPSCI*, July 3, 2012; ZTE, *Submission to HPSCI*, August 3, 2012; Ken Hu, “Huawei Open Letter.” <http://online.wsj.com/public/resources/documents/Huawei20110205.pdf> (accessed August 2, 2012). John Suffolk, Huawei’s Global Security Officer, previously served as the Chief Information Officer with the UK government at a time when the UK entered into its agreement with Huawei to set up the Cyber Security Evaluation Center (CSEC). Mr. Suffolk advocated for a cyber-security and supply-chain solution that would recognizing the issues as a global concern that must be addressed at an international level, preferably by an international standards-setting organization through which all products must pass. Mr. Suffolk also highlighted that in the present age, technology is moving faster than our ability to adapt our institutions. Key assumptions are that security requires a whole systems approach, and that all systems will be breached at some point. Thus, in Mr. Suffolk’s view, telecommunications companies and governments must manage the risk, focus on areas of most concern, instill diversity and adaptability, and learn to deal with the consequences. Mr. Suffolk acknowledged that Huawei’s desire to be an end-to-end provider for whole network solutions does not align with his proposed solutions to the supply-chain concerns, which depend on diversity of supply. HPSCI meeting with John Suffolk, February 23, 2012.

²³ Anderson, R., & Fuloria, S. *Certification and Evaluation: A Security Economics Perspective. Emerging Technologies and Factory Automation*, (2009).

²⁴ Ken Thompson, *Reflections on Trusting Trust. Turing Award Lecture*, (1984).

²⁵ Gerwin Klein, Formal Verification of an OS Kernel. *Symposium on Operating Systems Principles*. Big Sky, MT, USA: Association of Computing Machinery, (2009).

²⁶ Daniel Jackson, Martyn Thomas, and Lynette I. Millett, Eds. *Software for Dependable Systems: Sufficient Evidence? Committee on Certifiably Dependable Software Systems*, National Research Council. (National Academies Press, 2007.)

²⁷ Rules of the House of Representatives, 112th Congress, Rules 10(3)(m), 11.

²⁸ Understanding and developing a strategy to protect the country from Chinese cyber espionage in the United States is one of the obligations of U.S. counterintelligence professionals. Many reports have suggested that the Intelligence Community continues to struggle integrating and acting on its counterintelligence mission. As Michelle Van Cleave, former head of the National Counterintelligence Executive, has explained, “the U.S. government has been slow to appreciate the effects of foreign intelligence operations, much less to address the threats they pose to current U.S. foreign policy objectives or enduring national security interests.” Michelle Van Cleave, “Chapter 2: The NCIX and the National Counterintelligence Mission: What Has Worked, What Has Not, and Why,” in *Meeting Twenty-First Century Security Challenges*, 62.

Office of National Counterintelligence Executive, *Report to Congress on Foreign Economic Collection and Industrial Espionage*, “Foreign Spies Stealing US Economic Secrets in Cyberspace.”(October 2011, Washington, DC)

³⁰ In response to the Committee’s June 12, 2012, document request, ZTE provided one document: a summary of its cyber-security measures. Huawei provided no documents other than materials already on the company’s website or otherwise publicly released. After the September 13, 2012 hearing, Huawei provided a document labeled “Internal Compliance Program (ICP),” dated March 2012. That document summarizes Huawei’s internal policy with respect to trade control policies. Huawei provided no material that would allow the Committee to evaluate their compliance with or enforcement of that policy. Huawei also provided a copy of the publicly released paper entitled “Cyber Security Perspectives” prepared by John Suffolk, and Huawei’s public statement regarding its Commercial Operations in Iran.

³¹ House Permanent Select Committee on Intelligence, *Hearing on Investigation of the Security Threat Posed by Chinese Telecommunications Companies Huawei and ZTE*, 112th Congress, 2nd session (September 13, 2012).

³² Given the sensitivities involved, and to protect these witnesses from retaliation or dismissal, the Committee decided to keep the identities of these individuals confidential.

³³ As the U.S.-China Commission has highlighted, even the largely circumstantial evidence that known incidents appear state sponsored is compelling -- as the actors’ targeting often focuses on key defense and foreign-policy sources of information, which are of most concern to the state and not commercial entities. United States Congress, *2011 Annual Report of U.S.-China Economic and Security Review*. (2011, Washington DC: 59.)

³⁵ United States Congress, *2011 Annual Report of U.S.-China Economic and Security Review*. (2011, Washington DC: 59-60.)

³⁶ ZTE, *Submission to HPSCI*, July 3, 2012, 3.

³⁷ Discussion with PLA Piper, June 2012. Huawei, in its responses to Questions for the Record after the September 13, 2012, hearing, denied that there is any state-secret concern with their documentation. The Committee is left wondering, then, why Huawei has refused to provide internal documentation that could substantiate its claims. Moreover, Huawei’s failure to provide the list of individuals on Huawei’s Chinese Communist Party Committee is an example in which the Committee believes the state’s concerns with state secrets is particularly relevant. Huawei’s continuous failure to provide such information cannot be explained otherwise.

³⁸ Huawei Investment & Holding Co., Ltd., *2011 Annual Report*, 7.

³⁹ Ken Hu, “Huawei Open Letter.” <http://online.wsj.com/public/resources/documents/Huawei20110205.pdf> (accessed August 2, 2012).

⁴⁰ That report suggests that Huawei “was founded in 1988 by Ren Zhengfei, a former director of the PLA General Staff Department’s Information Engineering Academy, which is responsible for telecom research for the Chinese military. Huawei maintains deep ties with the Chinese military, which serves a multi-faceted role as an important customer, as well as Huawei’s political patron and research and development partner. Both the government and the military tout Huawei as a national champion, and the company is currently China’s largest, fastest-growing, and most impressive telecommunications-equipment manufacturer. Evan Medeiros et al., *A New Direction for China’s Defense Industry*, Rand Corporation: 218-219. http://www.rand.org/pubs/monographs/2005/RAND_MG334.pdf.

⁴¹ Ibid, 217-219

⁴² The Economist, “Huawei: The Company that Spooked the World,” *Economist*, August, 4, 2012. <http://www.economist.com/node/21559929> (accessed September 30, 2012).

⁴³ Juha Saarinen, “Analysis: Who Really Owns Huawei?,” *ITNews*, May 28, 2012.

⁴⁴ Ken Hu, “Huawei Open Letter.” <http://online.wsj.com/public/resources/documents/Huawei20110205.pdf> (accessed August 2, 2012).

⁴⁵ Richard McGregor, *The Party: The Secret World of China’s Communist Rulers*, 2010: 204.

⁴⁶ Huawei, *Submission to HPSCI*, July 3, 2012.

⁴⁷ House Permanent Select Committee on Intelligence, *Hearing on Investigation of the Security Threat Posed by Chinese Telecommunications Companies Huawei and ZTE*, 112th Congress, 2nd session (September 13, 2012).

⁴⁸ Huawei Investment & Holding Co., Ltd., *2011 Annual Report*, 2.

⁴⁹ Huawei, *September 25, 2012 Response to Questions for the Record*, at ____.

⁵⁰ Huawei, *September 25, 2012 Responses to Questions for the Record*, 6-7.

⁵¹ Interviews with Huawei officials, February 23, 2012.

⁵² Interviews with Huawei officials, February 23, 2012.

⁵³ Interviews with Huawei officials, February 23, 2012.

⁵⁴ Mike Rogers and Dutch Ruppersburg, letter to Huawei, June 12, 2012; Huawei, *letter to HPSCI*, “Response to June 12, 2012 Letter,” July 3, 2012.

⁵⁵ Huawei, *Documents Provided in Advance of February 23, 2012 entitled Shareholder Agreements*.

⁵⁶ John Lee, “The Other Side of Huawei,” *Business Spectator*, March 30, 2012.

⁵⁷ United States Congress, *2011 Annual Report of U.S.-China Economic and Security Review*. (2011, Washington DC: 59)

⁵⁸ Ibid.

⁵⁹ House Permanent Select Committee on Intelligence, *Hearing on Investigation of the Security Threat Posed by Chinese Telecommunications Companies Huawei and ZTE*, 112th Congress, 2nd session (September 13, 2012).

⁶⁰ Huawei, *Submission to House Permanent Select Committee on Intelligence*, July 3, 2012, 1.

⁶¹ Ibid.

⁶² Ibid.

⁶³ Huawei, *July 2, 2012 Submission*, 7-15

⁶⁴ Highlighting that as China moved from a pure control economy in the 1990s, Chinese companies experienced particular difficulties raising capital in foreign capital markets, including the “most sensitive of all, how would they explain the role of the internal party bodies, which for years had run companies, free of any of the inconvenient structuring of corporate reporting and governance rules.” Richard McGregor, *The Party: The Secret World of China’s Communist Rulers*, 2010: 47; See John Lee, “The Other Side of Huawei,” *Business Spectator*, March 30, 2012

⁶⁵ Huawei, *Submission to House Permanent Select Committee on Intelligence*, July 3, 2012, 2.

⁶⁶ Ibid.

⁶⁷ See John Lee, “The Other Side of Huawei,” *Business Spectator*, March 30, 2012; Richard McGregor, *The Party: The Secret World of China’s Communist Rulers*, 2010.

⁶⁸ Richard McGregor, *The Party: The Secret World of China’s Communist Rulers*, 2010: 72.

⁶⁹ Meeting with Mr. Ren, May 23, 2012.

⁷⁰ Huawei, *Submission to House Permanent Select Committee on Intelligence*, July 3, 2012.

⁷¹ Huawei officials stated that China had cancelled ranking system at the time. HPSCI Interviews with Huawei officials, February 23, 2012.

⁷² Huawei officials suggested that the rumors that Mr. Ren is a former PLA General is the result of confusion with Julong, another Chinese telecommunications company and state-owned enterprise whose President is a Major General in the PLA. HPSCI Interviews with Huawei officials, February 13, 2012.

⁷³ Huawei, *September 25, 2012 Responses to HPSCI Questions for the Record*, 8.

⁷⁴ Huawei, *September 25, 2012 Responses to HPSCI Questions for the Record*, 8.

⁷⁵ Huawei asserted that Chen Jinyang, who invested 3,500 RMB, was a 26-year-old manager at the Chinese Trade Department.

⁷⁶ Interviews with Huawei officials, February 23, 2012.

⁷⁷ Interviews with Huawei officials, February 23, 2012.

⁷⁸ Interview with Ken Hu, February 23, 2012.

⁷⁹ Scholars of the Chinese political economy suggest that national champions are those chosen by China to be supported both financially and otherwise by the state because of the strategic importance of the sector and the company to China’s national interests. See John Lee, “The Other Side of Huawei,” *Business Spectator*, March 30, 2012

⁸⁰ Huawei, *Submission to House Permanent Select Committee on Intelligence*, July 3, 2012, 19.

⁸¹ Ibid.

⁸² Interviews with Huawei officials, February 23, 2012; Huawei presentation, February 23, 2012.

⁸³ Interviews with Huawei officials, February 23, 2012

⁸⁴ Huawei, *Submission to House Permanent Select Committee on Intelligence*, July 3, 2012, 19-20.

⁸⁵ Mike Rogers and Dutch Ruppersburg, letter to Huawei, June 12, 2012, 6.

⁸⁶ Huawei, *Submission to House Permanent Select Committee on Intelligence*, July 3, 2012, 19-20.

⁸⁷ Phone conversations with Huawei representatives, June 2012.

⁸⁸ Huawei, *Submission to House Permanent Select Committee on Intelligence*, July 3, 2012, 20-21.

⁸⁹ John Lee, "The Other Side of Huawei," *Business Spectator*, March 30, 2012.

⁹⁰ The Economist, "Huawei: The Company that Spooked the World," *Economist*, August, 4, 2012.

<http://www.economist.com/node/21559929> (accessed September 30, 2012);

⁹¹ House Permanent Select Committee on Intelligence, *Hearing on Investigation of the Security Threat Posed by Chinese Telecommunications Companies Huawei and ZTE*, 112th Congress, 2nd session (September 13, 2012).

⁹² Huawei, *Slide Presentation dated November 2011*, 8.

⁹³ Huawei, *Responses to HPSCI Questions for the Record*, September 25, 2012, 1.

⁹⁴ Ibid.

⁹⁵ Ibid.

⁹⁶ Interviews with Huawei officials, February 23, 2012

⁹⁷ Huawei, *Corporate Presentation*, February 23, 2012, 26.

⁹⁸ Huawei, *Submission to House Permanent Select Committee on Intelligence*, July 3, 2012, 2.

⁹⁹ Huawei, *Corporate Presentation*, February 23, 2012, 27.

¹⁰⁰ Huawei, *Responses to HPSCI Questions for the Record*, September 25, 2012, 2.

¹⁰¹ Interviews with Huawei officials, February 23, 2012.

¹⁰² House Permanent Select Committee on Intelligence, *Hearing on Investigation of the Security Threat Posed by Chinese Telecommunications Companies Huawei and ZTE*, 112th Congress, 2nd session (September 13, 2012).

¹⁰³ Huawei, *Submission to House Permanent Select Committee on Intelligence*, July 3, 2012, 21.

¹⁰⁴ Interviews with Huawei officials, February 23, 2012.

¹⁰⁵ Ren Zhengfei, speech at Huawei BT Division & Huawei UK, June 30, 2007, quoted in Huawei magazine *Improvement*, Issue 58.

¹⁰⁶ The Commerce Department, working with the Defense Department, has sought information from the private sector to better understand the entire scope of cyber-risks facing the country's critical telecommunication infrastructure. The Commerce issued a survey under the Defense Production Act to dozens of U.S. based companies to gather better information on the security of their networks. The review of that information is still ongoing.

¹⁰⁷ The Committee has offered on numerous occasions to provide Huawei an opportunity to provide the information the Committee needs to evaluate the security of U.S. networks in a closed forum or under an agreement to provide such information confidentially. Huawei has continuously refused to accept any such offer, option instead to simply assert that such details are confidential. The Committee intends to continue evaluating these issues and plans to approach Huawei in the future for more details on these contracts to fulfill the Committee's duty to evaluate the risk posed by these firms.

¹⁰⁸ House Committee on Foreign Affairs, *Hearing on Unfair Trade Practices against the US*, 112th Congress, 2nd session (July 19, 2012).

¹⁰⁹ Interview with Huawei officials, February 23, 2012.

¹¹⁰ Interview with Employees.

¹¹¹ John Lee, "The Other Side of Huawei," *Business Spectator*, March 30, 2012.

¹¹² Interview with Huawei officials, February 23, 2012.

¹¹³ Huawei, *Submission to House Permanent Select Committee on Intelligence*, July 3, 2012.

¹¹⁴ Interview with Huawei Employees.

¹¹⁵ Interview with Huawei Employees.

¹¹⁶ Interview with industry experts.

¹¹⁷ Huawei representatives admitted to Committee staff that using this presentation was in violation of McKinsey's copyright protections, and that McKinsey and Huawei have no business relationship thus undermining any claim that Huawei had a right to use the slide. Huawei, *Slide Presentation dated November 2011*, 8 (using McKinsey & Co. material).

¹¹⁸ Interview with Huawei Officials, February 13, 2012.

¹¹⁹ Ibid.

¹²⁰ Marguerite Reardon, "Huawei Admits Copying," *Light Reading*, March 25, 2003.

http://www.lightreading.com/document.asp?doc_id=30269 (accessed on August 13, 2012)

¹²¹ Ibid.

¹²² House Permanent Select Committee on Intelligence, *Hearing on Investigation of the Security Threat Posed by Chinese Telecommunications Companies Huawei and ZTE*, 112th Congress, 2nd session (September 13, 2012).

¹²³ Huawei, *Submission to House Permanent Select Committee on Intelligence*, July 3, 2012, 6.

¹²⁴ Ibid.

¹²⁵ Ibid, 5-6.

¹²⁶ Ibid, 3-4.

¹²⁷ Ibid, 3.

¹²⁸ Interviews with Huawei officials, February 23, 2012.

¹²⁹ Huawei, *September 25, 2012 Responses to Questions for the Record*, 12.

¹³⁰ Ibid.

¹³¹ Internal Huawei email, dated July 1, 2011.

¹³² Ibid.

¹³³ Interviews with former Huawei employees.

¹³⁴ Interviews with former Huawei employees.

¹³⁵ Huawei, *Slide Presentation dated November 2011*, 8.

¹³⁶ ZTE August 3, 2012 submission, at 12-17.

¹³⁷ ZTE, *Submissions to HPSCI*, August 3, 2012, 23.

¹³⁸ ZTE, *2011 Annual Report*, 68-69.

¹³⁹ "The national '12th Five Year Plan' has provided driving force for the further development of the domestic telecommunications industry." ZTE, *2011 Annual Report*, 69.

¹⁴⁰ Meeting with ZTE officials, April 12, 2012, Shenzhen, China.

¹⁴¹ ZTE, *Submissions to HPSCI*, July 3, 2012.

¹⁴² Ibid, 4.

¹⁴³ Ibid.

¹⁴⁴ As a report commissioned by the U.S. China-Commission stated: "The IT sector in China can be considered a hybrid defense industry, able to operate with success in commercial markets while meeting the demands of its military customers. The Chinese telecommunications market is heavily influenced by its largest domestic members—such as hardware and networking giants Huawei Shenzhen Technology Company, Zhongxing Telecom (ZTE), and Datang Telecom Technology Co., Limited. These companies and some smaller players are not always directly linked to the PLA or C4ISR modernization because of their strong domestic and international commercial orientation. The digital triangle model, however, allows them to benefit directly from a background network of state research institutes and government funding in programs that do have affiliation or sponsorship of the PLA." Northrop Grumman Corp, *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage*, prepared for U.S.-China Economic and Security Review Commission, March 7, 2012, 69.

¹⁴⁵ ZTE, *Submissions to HPSCI*, July 3, 2012, 2.

¹⁴⁶ Ibid, 9

¹⁴⁷ Ibid.

¹⁴⁸ Ibid, 4.

¹⁴⁹ House Permanent Select Committee on Intelligence, *Hearing on Investigation of the Security Threat Posed by Chinese Telecommunications Companies Huawei and ZTE*, 112th Congress, 2nd session (September 13, 2012).

¹⁵⁰ John Merrigan, letter to Katie Wheelbarger, September 28, 2012.

¹⁵¹ Affidavit of Timothy Steinert, at para. 6.

¹⁵² ZTE, *Submissions to HPSCI*, August 3, 2012, 5.

¹⁵³ Meeting with ZTE officials, April 12, 2012, Shenzhen, China.

¹⁵⁴ Ibid.

¹⁵⁵ House Permanent Select Committee on Intelligence, *Hearing on Investigation of the Security Threat Posed by Chinese Telecommunications Companies Huawei and ZTE*, 112th Congress, 2nd session (September 13, 2012).

¹⁵⁶ Ellen Nakashima, “Chinese telecom firm ZTE probed for alleged sale of U.S. surveillance equipment to Iran,” *Washington Post*, July 13, 2012. http://www.washingtonpost.com/world/national-security/chinese-telecom-firm-zte-probed-for-alleged-sale-of-us-surveillance-equipment-to-iran/2012/07/13/gJQA6mKUiW_story.html.

¹⁵⁷ House Permanent Select Committee on Intelligence, *Hearing on Investigation of the Security Threat Posed by Chinese Telecommunications Companies Huawei and ZTE*, 112th Congress, 2nd session (September 13, 2012).

¹⁵⁸ ZTE, *Submissions to HPSCI*, April 2012, 4.

¹⁵⁹ Ibid.

¹⁶⁰ Ibid.

¹⁶¹ ZTE, *Submissions to HPSCI*, July 3, 2012, 17.

EXHIBIT B

RECEIVED - CLERK
U.S. DISTRICT COURT
EASTERN DISTRICT OF TEXAS

IN THE UNITED STATES DISTRICT COURT

03 JAN 22 PM 7:50 FOR THE EASTERN DISTRICT OF TEXAS

EASTERN DISTRICT
OF TEXAS

MARSHALL DIVISION

FILED
U. S. DISTRICT COURT
EASTERN DISTRICT OF TEXAS

JAN 22 2003

DAVID MALAND, CLERK
By Deputy *Blunder*

CISCO SYSTEMS, INC. AND
CISCO TECHNOLOGY, INC.

Plaintiffs,

v.

HUAWEI TECHNOLOGIES, CO., LTD.,
HUAWEI AMERICA, INC. AND
FUTUREWEI TECHNOLOGIES, INC.,

Defendants.

CIVIL ACTION NO. [2-03C] - 027

COMPLAINT AND JURY DEMAND *TJW*

For its complaint against Defendants Huawei Technologies Co., Ltd. (“Huawei”), Huawei America, Inc. (“Huawei America”) and FutureWei Technologies, Inc. (“FutureWei”) (collectively “Defendants”), Plaintiffs Cisco Systems, Inc. (“Cisco Systems”) and Cisco Technology, Inc. (“Cisco Technology”) (collectively “Cisco”) allege as follows:

I. NATURE OF THE ACTION

1. This is an action arising from Defendants’ systematic and wholesale infringement of Cisco’s intellectual property. Huawei, a Chinese company, and its wholly owned United States subsidiaries, Huawei America and FutureWei, manufacture and offer for sale a line of network routers designed to compete with Cisco’s network routers. Unlike Cisco, however, which invested substantially in the development of its own proprietary router technology and software, Huawei has chosen to misappropriate and infringe Cisco’s intellectual property in an attempt to develop a cheaper, inferior router which Huawei claims is compatible with Cisco’s routers. In doing so, Huawei and its U.S. subsidiaries have shown a complete disregard for Cisco’s intellectual property rights and the laws which protect those rights. The extent of Defendants’ copying and misappropriation of Cisco’s intellectual property is

staggering. Defendants have copied Cisco's patented technologies; they have copied the copyrighted user interface for Cisco's routers; they have made verbatim copies of whole portions of Cisco's user manuals; and there is overwhelming evidence that they unlawfully gained access to Cisco's source code and copied it as the basis for the operating system for their knock-off routers. Cisco brings this action to enjoin this wholesale theft of its valuable intellectual property and recover the substantial damages it has incurred from Defendants' illegal conduct.

II. PARTIES

2. Cisco Systems is a California corporation with its principal place of business in San Jose, California. It is a worldwide leader in the development, manufacture and sale of computer networking products.

3. Cisco Technology is a California corporation with its principal place of business in San Jose, California. Cisco Technology is a wholly-owned subsidiary of Cisco Systems.

4. On information and belief, Huawei is a foreign corporation with its principal place of business in the Peoples Republic of China. It is a multi-billion dollar company that conducts business throughout the world in the manufacture and sale of network and telecommunications equipment. On information and belief, Huawei conducts business in this judicial district through FutureWei and/or Huawei America.

5. FutureWei is a corporation organized and existing under the laws of the State of Texas with its principal place of business at 1700 Alma Drive, Plano, Texas. On information and belief, FutureWei is a wholly owned subsidiary of Huawei. FutureWei is present in and conducts business in this judicial district. In addition to its Plano office, FutureWei also maintains offices in San Jose, California and Reston, Virginia. FutureWei's registered agent is:

Rongxin Chong
1700 Alma Drive, Suite 500
Plano, Texas 75075

6. Huawei America is a corporation organized and existing under the laws of the State of California with its principal place of business in San Jose, California. On information and belief, Huawei America is a wholly owned subsidiary of Huawei. Huawei America is present in and conducts business in this judicial district. In addition to its San Jose office, Huawei America also maintains a sales office in Plano, Texas. Huawei America's registered agent is:

James Yan
3772 Sun West Terrace
Fremont, CA 94555

III. JURISDICTION AND VENUE

7. Defendants transact business and are found in this judicial district through regular business conduct and activity that includes, among other things, the following:

- a. Huawei offers for sale in this district the network routers and related software which are alleged in this action to infringe Cisco's intellectual property rights.
- b. Huawei already has made commercial sales in the United States of the network routers which are alleged in this action to infringe Cisco's intellectual property rights, including sales originated from the sales office in Plano, Texas.
- c. Huawei and FutureWei each operate a website for the purpose of promoting Huawei products, including the network routers, switches and other network products that use the software alleged to infringe Cisco's intellectual property rights. The Huawei and FutureWei websites can be accessed by customers, potential customers and others located in this district for information about the allegedly infringing routers and other Huawei products, as well as employment opportunities with Huawei's interests in the United States. The infringing computer software created by Defendants through the violation of Cisco's rights, referred to as "VRP," and the infringing user manuals created by Defendants through the violation of Cisco's rights can be downloaded by residents of this district through the Huawei website.

d. Huawei operates a research and development facility in this district, in Plano, and has actively recruited residents of this district and elsewhere for employment at that facility.

e. Huawei has incorporated a subsidiary in Texas (FutureWei) for the purpose of doing business in the United States. The FutureWei sales office in Plano, Texas promotes and sells the infringing routers which are the subject of this action and otherwise conducts business in this judicial district.

f. Huawei has created a California subsidiary (Huawei America) for the purpose of doing business in the United States. Huawei America also maintains a sales office in Plano, Texas, through which it regularly engages in activities to promote and sell the infringing routers and otherwise conducts business in this judicial district.

g. Huawei, FutureWei and Huawei America are accused of committing a number of illegal acts and infringements of Cisco's intellectual property, the harmful effect of which is felt in this judicial district where Cisco sells a substantial volume of products and maintains a substantial research and development facility.

8. The Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C. §§ 1331, 1338(a) and (b), and 1367 and the doctrine of supplemental jurisdiction.

9. Venue is proper in this judicial district pursuant to 28 U.S.C. §§ 1391 and 1400 because (1) Huawei is a foreign corporation subject to personal jurisdiction in this district, (2) Defendants reside and may be found in this judicial district, (3) the acts of infringement and misappropriation alleged herein were committed in this judicial district, (4) Defendants have a regular and established place of business in this district, and/or (5) a substantial part of the events giving rise to the claims occurred in this judicial district.

IV. FACTUAL BACKGROUND

10. Cisco provides a broad line of hardware and software solutions for transporting data, voice, and video over networks and throughout the Internet. Included in the equipment Cisco provides are network routers, switches, and devices that enable data and

information to be transported from one network to another – locally, regionally and internationally. Routers and switches are the backbone of Internet traffic, routing packets of data as they are transported from sender to recipient. For example, the transmission of an email message from Dallas, Texas to Hong Kong will pass through multiple routers or switches as the packets of information comprising the message pass from one network to another. The science of routing packets of data through networks is complex and challenging and requires tremendous innovation and technological development to assure that messages are sent quickly and securely and arrive at their intended destination. As a pioneer in this area, Cisco has achieved widespread renown for the technological superiority, convenience and security of its routers, which in turn has facilitated the amazing growth of computer networks and the Internet.

11. Cisco came to its position of technological leadership by hard work and substantial research and development investment. As a result of its endeavors, Cisco has created valuable intellectual property in the form of patents, copyrights, trademarks and trade secrets that protect the valuable technology it has created. Cisco is the owner of a number of key patents covering the operation of its routers and the particularized manner in which they function. One of the core technologies contained in every Cisco router is called the Cisco Internetwork Operating System (“IOS Software Programs”), a proprietary computer program that manages the routing of packets through the router or switch. The IOS Software Programs are the product of countless man-hours of software design and programming by Cisco employees and contractors.

12. Defendants recently introduced for sale in the United States a line of routers referred to as “Quidway routers” which, on information and belief, it has promoted as operating virtually identically as Cisco routers but costing less than Cisco routers. On information and belief, Huawei sells the same or similar infringing routers in a number of foreign countries, the exact identities of which Cisco expects to learn through discovery. On information and belief, Defendants promote their Quidway routers by claiming they can replace a Cisco router without any loss of performance or security. While Defendants’ claim of interoperability are dubious, it is apparent that in their attempt to produce a Cisco “clone,” Defendants engaged

in wholesale theft of Cisco's intellectual property. That theft includes the adoption of Cisco's patented processes, the systematic copying of Cisco's copyrighted Command Line Interface, the copying of Cisco's proprietary IOS source code, and the systematic copying of Cisco's user manuals. Huawei's Vice President, Fei Min, recently admitted that "all the world's leading equipment suppliers are our learning models." The evidence shows unequivocally that the "learning" was in fact blatant copying and misappropriation, undertaken in complete disregard of Cisco's intellectual property rights.

Cisco's Copyright Protection.

13. Cisco Technology has duly recorded in the United States Copyright Office registrations protecting Cisco's IOS Software Programs, its Command Line Interface, and its User Manuals. Cisco Technology is the owner of the registered copyrights in each of the following computer programs and their corresponding user manuals, each of which substantially consists of original material (hereafter referred to as "Cisco's Copyrighted Works"). The following Cisco's Copyrighted Works consist of their respective computer code ("IOS Software Programs"), the Command Line Interface and corresponding screen displays ("CLI"), and the corresponding IOS user manuals ("IOS Manuals"):

- a. Cisco Internetwork Operating System Version 11.0, Reg. No. TXu-1-036-057 (Ex. A)
- b. Cisco Internetwork Operating System Version 11.1, Reg. No. TXu-1-048-569 (supplementing TX-5-531-435) (Ex. B)
- c. Cisco Internetwork Operating System Version 11.2, Reg. No. TXu-1-036-063 (Ex. C)
- d. Cisco Internetwork Operating System Version 11.3, Reg. No. TXu-1-036-062 (Ex. D)
- e. Cisco Internetwork Operating System Version 12.0, Reg. No. TXu-1-036-064 (Ex. E)

- f. Cisco Internetwork Operating System Version 12.1, Reg. No. TXu-1-036-066 (Ex. F)
- g. Cisco Internetwork Operating System Version 12.2, Reg. No. TXu-1-036-065 (Ex. G)

14. For each of the foregoing works, Cisco Technology complied in all respects with the Copyright Act and all other laws of the United States governing copyrights, and has received Certificates of Registration from the Register of Copyrights.

Copying of Command Line Interface.

15. A key component of the copyrighted IOS Software Programs is the “Command Line Interface” or “CLI.” The CLI is the user interface by which users of Cisco routers communicate with the routers. Just as a computer user must communicate instructions to a computer (e.g., copy a file), the Information Technology (“IT”) manager must communicate with routers in order to configure and manage them. For Cisco routers the interaction between the IT manager and the router is facilitated by a unique Command Line Interface, an elaborate structure of textual commands that the IT manager must learn in order to “talk” to the router. Each command corresponds to a function that can be performed by the router. When the command is entered by the human operator, the router performs the function associated with that particular command.

16. Cisco’s CLI is a unique, expressive work that has been developed over many years of creative endeavor. Other manufacturers of network routers have their own command line interfaces that differ from Cisco’s, both in terms of the particular commands and in the organization of those commands. When developing a router interface, the software developer has a range of creative choices in deciding what textual commands to compose, the definitions assigned to the commands, and the overall structure of the interface. Cisco’s CLI represents its own original expression of one way to provide this communication.

17. Defendants have engaged in wholesale copying of Cisco’s CLI. Because the CLI can be visually observed during the operation of a router and is published in Cisco’s user

manuals, Defendants would have had no difficulty in gaining access to the CLI. A comparison of the command line interface of the operating system for the Quidway routers, switches and other products that use VRP, and Cisco's CLI reveals repeated incidents of slavish copying. For example, the following chart shows two of the many areas in which commands were copied by Defendants.

CISCO'S IOS <u>HSRP Commands</u>	DEFENDANTS' VRP <u>HSRP Commands</u>
standby authentication	standby authentication
standby ip	standby ip
standby preempt	standby preempt
standby priority	standby priority
standby timers	standby timers
standby track	standby track
standby use-bia	standby use-bia
standby mac-address <address>	standby use-ovmac
show standby	show standby
debug standby	debug standby
 <u>PQ Commands</u>	 <u>PQ Commands</u>
priority-group	priority-group
priority-list default	priority-list default
priority-list interface	priority-list interface
priority-list protocol	priority-list protocol
priority-list queue-limit	priority-list queue-limit
show queuing priority	show queuing priority
debug priority-queue	debug priority

18. So much of the Cisco CLI is duplicated in the Defendants' interface that an IT manager familiar with the Cisco CLI would not have to be re-trained in order to operate one of Huawei's Quidway routers, switches or products that use VRP. As a result of its extensive copying of the Cisco CLI, Defendants can promote their Quidway routers, switches and products that use VRP by convincing Cisco customers that they will not have to learn a new command line interface if they purchase Defendants' products. On information and belief, Defendants have informed customers that IT managers familiar with Cisco routers will not need additional training to manage Defendants' products. As one Huawei distributor declared, he was "impressed by the ability of a Cisco-trained engineer to take a Huawei product out of the box and use it." By choosing copyright infringement over independent development, Defendants are attempting to compete with Cisco by stealing Cisco's innovations instead of creating their own as well as avoiding the process of training potential users in a separate interface.

Copying of IOS Source Code.

19. Cisco is informed and believes and therefore alleges that Defendants have copied substantial portions of the IOS Software Programs source code. The operating system for the Quidway routers is known as "VRP," which stands for Versatile Routing Platform. The VRP program contains telltale similarities to the IOS Software Programs indicating that Defendants had access to the proprietary IOS Software Programs source code and used some or all of the source code in the creation of VRP.

20. The IOS Software Programs source code contains thousands of "text strings," distinctive textual statements written into the software by the programmers to convey information about the tasks to be performed by the software. Software which is independently developed will have unique text strings organized in a unique sequence or order. An analysis of Defendants' VRP code reveals that it contains large portions of text strings that are identical or substantially similar to the text strings from the IOS Software Programs, both in terms of the phrasing of the text strings and the sequence in which they appear. This level of identicity cannot be explained by either coincidence or independent development on the part of Huawei. It

points inescapably to one conclusion: Defendants had access to Cisco's proprietary IOS source code and copied that source code in the creation of Defendants' VRP.

21. At various points in time, the IOS Software Programs have had minor bugs that do not affect the fundamental functions of the program but represent idiosyncratic ways in which the program was written. Because they stand as unusual anomalies, these bugs serve as telltale fingerprints if they appear in other computer programs. Just as a school teacher can determine copying from the existence of a shared mistake among student papers, Cisco has discovered the presence of a "bug" in the Defendants' VRP software, which can only be explained by Defendants' unlawful access to and use of the IOS Software Programs source code.

22. Cisco has never made its IOS source code available to Defendants nor has it ever authorized anyone else to do so. Cisco is informed and believes and therefore alleges that Defendants obtained access to Cisco's IOS source code or portions thereof by improper means, that Defendants had reason to know that the source code was confidential to Cisco, and that Defendants had reason to know that their access to the source code was not authorized by Cisco. On information and belief, Defendants have exercised dominion and control over Cisco's IOS source code, which is in the form of one or more computer files (i.e., one or more documents), in an unlawful and unauthorized manner to the exclusion of and inconsistent with Cisco's rights. Defendants' possession of Cisco's IOS source code is tantamount to a refusal after demand.

Copying of Cisco's User Manuals.

23. Cisco provides the IOS Manuals to its customers to assist them in the operation of Cisco's routers. These manuals describe in detail the operation of the Cisco routers, the CLI and how to configure the routers for use in network operation. Cisco has invested thousands of man-hours in the preparation of the IOS Manuals, each of which is protected from unlawful copying under the Copyright Laws of the United States and other countries.

24. Defendants make available to customers and prospective customers user manuals that explain the function of its Quidway routers, switches, and other products that use VRP. In creating Defendants' user manuals, Defendants have copied extensively from the IOS

Manuals. In many cases, Defendants have copied whole paragraphs of text from the IOS Manuals, sometimes changing a word here or there in an attempt to mask their flagrant plagiarism. Defendants also have copied the organization and structure of the IOS Manuals so that the overall appearance of Defendants' manuals is substantially similar to the IOS Manuals. Attached as Exhibit H is an example of Defendants' copying of Cisco's copyrighted user manuals.

Patent Infringement.

25. In addition to the unlawful conduct described above, Defendants also have infringed Cisco's patented processes and methods in their attempt to create a router that replicates the functionality of Cisco's routers. In particular, Defendants have infringed no less than five Cisco patents through their incorporation of patented and proprietary Cisco technology in Quidway routers, switches, and other network devices that use VRP. These infringements were blatant and willful and were part of Defendants' overall plan to misappropriate Cisco's technology.

Adoption of Cisco's Nomenclature and Model Numbers.

26. In addition to the theft of Cisco's technology, Defendants have taken steps to mislead customers into believing that their Quidway routers are comparable to and completely interchangeable with Cisco routers.

27. Defendants have adopted a product numbering scheme for their router products that is substantially the same as Cisco's numbering scheme. Defendants have adopted other Cisco nomenclature as well, such as Cisco's acronym for its security products (i.e., "SAFE"). Huawei refers to its security products as SAFE. The title Cisco applies to engineers who are certified in operating Cisco's routers, "Certified Cisco Internetworking Experts" or "CCIE" has also been appropriated by Defendants in their use of the term "Huawei Certified Internetworking Experts" or "HCIE." Given the wide range of model numbers and nomenclature from which Defendants could have chosen, their decision to mimic Cisco's naming conventions is further evidence of Defendants' unlawful scheme to knock off Cisco's technology and mislead

customers into believing that the products are interchangeable without any loss of performance, security or reliability.

V. COUNT ONE

(Patent Infringement—'032 Patent)

28. Plaintiff Cisco realleges and repeats the allegations of paragraphs 1 through 27 above.

29. On February 11, 1992, the United States Patent and Trademark Office duly and legally issued United States Letters Patent No. 5,088,032 (the “‘032 patent”) entitled “METHOD AND APPARATUS FOR ROUTING COMMUNICATIONS AMONG COMPUTER NETWORKS.” Cisco Technology holds legal title to the ‘032 patent. By virtue of a license, Cisco Systems has all substantial rights in the ‘032 patent, including the right to sue for infringement of the ‘032 patent.

30. Defendants have been and are infringing the ‘032 patent within this district and elsewhere in the United States by making, using, selling, importing, distributing or offering for sale products that infringe one or more of the claims of the ‘032 patent.

31. Defendants are contributorily infringing the ‘032 patent within this district and elsewhere in the United States by making, using, selling, importing, distributing or offering for sale in the United States materials and/or apparatus for use in practicing the inventions set forth in the ‘032 patent, that they know to be especially made or especially adapted for use in infringement of the invention embodied in the ‘032 patent. On information and belief, these materials and/or apparatus have no substantial non-infringing use in commerce.

32. Defendants are inducing infringement of the ‘032 patent within this district and elsewhere in the United States by instructing in the use of materials and/or apparatus that infringe one or more of the claims of the ‘032 patent.

VI. COUNT TWO

(Patent Infringement—'599 Patent)

33. Plaintiff Cisco realleges and repeats the allegations of paragraphs 1 through 32 above.

34. On December 5, 1995, the United States Patent and Trademark Office duly and legally issued United States Letters Patent No. 5,473,599 (hereinafter the "'599 patent"), entitled "STANDBY ROUTER PROTOCOL." Cisco Technology holds legal title to the '599 patent. By virtue of a license, Cisco Systems has all substantial rights in the '599 patent, including the right to sue for infringement of the '599 patent.

35. Defendants have been and are infringing the '599 patent within this district and elsewhere in the United States by making, using, selling, importing, distributing or offering for sale products that infringe one or more of the claims of the '599 patent.

36. Defendants are contributorily infringing the '599 patent within this district and elsewhere in the United States by making, using, selling, importing, distributing or offering for sale in the United States materials and/or apparatus for use in practicing the inventions set forth in the '599 patent, that they know to be especially made or especially adapted for use in infringement of the inventions embodied in the '599 patent. On information and belief, these materials and/or apparatus have no substantial non-infringing use in commerce.

37. Defendants are inducing infringement of the '599 patent within this district and elsewhere in the United States by instructing in the use of materials and/or apparatus that infringe one or more of the claims of the '599 patent.

VII. COUNT THREE

(Patent Infringement—'704 Patent)

38. Plaintiff Cisco realleges and repeats the allegations of paragraphs 1 through 37 above.

39. On May 21, 1996, the United States Patent and Trademark Office duly and legally issued United States Letters Patent No. 5,519,704 (hereinafter the "'704 patent"), entitled

“RELIABLE TRANSPORT PROTOCOL FOR INTERNETWORK ROUTING.” Cisco Technology holds legal title to the ’704 patent. By virtue of a license, Cisco Systems has all substantial rights in the ’704 patent, including the right to sue for infringement of the ’704 patent.

40. Defendants have been and are infringing the ’704 patent within this district and elsewhere in the United States by making, using, selling, importing, distributing or offering for sale products that infringe one or more of the claims of the ’704 patent.

41. Defendants are contributorily infringing the ’704 patent within this district and elsewhere in the United States by making, using, selling, importing, distributing or offering for sale in the United States materials and/or apparatus for use in practicing inventions set forth in the ’704 patent, that they know to be especially made or especially adapted for use in infringement of the inventions embodied in the ’704 patent. On information and belief, these materials and/or apparatus have no substantial non-infringing use in commerce.

42. Defendants are inducing infringement of the ’704 patent within this district and elsewhere in the United States by instructing in the use of materials and/or apparatus that infringe one or more of the claims of the ’704 patent.

VIII. COUNT FOUR

(Patent Infringement—’718 Patent)

43. Plaintiff Cisco realleges and repeats the allegations of paragraphs 1 through 42 above.

44. On August 1, 2000, the United States Patent and Trademark Office duly and legally issued United States Letters Patent No. 6,097,718 (hereinafter the “’718 patent”), entitled “SNAPSHOT ROUTING WITH ROUTE AGING.” Cisco Technology holds legal title to the ’718 patent. By virtue of a license, Cisco Systems has all substantial rights in the ’718 patent, including the right to sue for infringement of the ’718 patent.

45. Defendants have been and are infringing the ’718 patent within this district and elsewhere in the United States by making, using, selling, importing, distributing or offering for sale products that infringe one or more of the claims of the ’718 patent.

46. Defendants are contributorily infringing the '718 patent within this district and elsewhere in the United States by making, using, selling, importing, distributing or offering for sale in the United States materials and/or apparatus for use in practicing the inventions set forth in the '718 patent, that they know to be especially made or especially adapted for use in infringement of the inventions embodied in the '718 patent. On information and belief, these materials and/or apparatus have no substantial non-infringing use in commerce.

47. Defendants are inducing infringement of the '718 patent within this district and elsewhere in the United States by instructing in the use of materials and/or apparatus that infringe one or more of the claims of the '718 patent.

IX. COUNT FIVE

(Patent Infringement—'251 Patent)

48. Plaintiff Cisco realleges and repeats the allegations of paragraphs 1 through 47 above.

49. On December 4, 2001, the United States Patent and Trademark Office duly and legally issued United States Letters Patent No. 6,327,251 (hereinafter the "'251 patent"), entitled "SNAPSHOT ROUTING." Cisco Technology holds legal title to the '251 patent. By virtue of a license, Cisco Systems has all substantial rights in the '251 patent, including the right to sue for infringement of the '251 patent.

50. Defendants have been and are infringing the '251 patent within this district and elsewhere in the United States by making, using, selling, importing, distributing or offering for sale products that infringe one or more of the claims of the '251 patent.

51. Defendants are contributorily infringing the '251 patent within this district and elsewhere in the United States by making, using, selling, importing, distributing or offering for sale in the United States materials and/or apparatus for use in practicing the inventions set forth in the '251 patent, that they know to be especially made or especially adapted for use in infringement of the inventions embodied in the '251 patent. On information and belief, these materials and/or apparatus have no substantial non-infringing use in commerce.

52. Defendants are inducing infringement of the '251 patent within this district and elsewhere in the United States by instructing in the use of materials and/or apparatus that infringe one or more of the claims of the '251 patent.

X. COUNT SIX

(Copyright Infringement – IOS source code and CLI)

53. Cisco alleges and incorporates by reference the allegations in paragraphs 1 through 52 above.

54. Defendants have infringed and, unless enjoined in this action, will continue to infringe Cisco's Copyrighted Works by, among other things:

- (a) Copying substantial portions of the code of the IOS Software Programs;
- (b) Copying substantial portions of the CLI;
- (c) Distributing works containing material copied from the IOS Software Programs and CLI; and
- (d) Creating derivative works based on the IOS Software Programs and CLI.

55. Defendants' copying and distribution of the IOS Software Programs and CLI and the creation of unauthorized derivative works constitute willful infringement under the Copyright Act. By reason of Defendants' acts of infringement, Cisco has suffered and will continue to suffer, unless Defendants' infringement is enjoined, irreparable injury that cannot be adequately remedied at law. Because of such willful infringement, Cisco is entitled to enhanced damages and an award of its attorneys fees and costs pursuant to the Copyright Act.

56. Defendants' unauthorized copying and distribution of the IOS Software Programs and CLI and the creation of unauthorized derivative works constitute willful infringement under the copyright laws (or laws extending similar protection) of the foreign countries in which Defendants have copied, sold or distributed their infringing works. By reason of these acts of infringement, Cisco has suffered and will continue to suffer, unless Defendants'

infringement is enjoined, irreparable injury that cannot be adequately remedied at law. The exact foreign countries in which defendants have copied, sold or distributed their infringing works, and the extent of that illegal conduct, are not presently known to Cisco and can be learned only upon appropriate discovery from defendants. Cisco reserves the right, upon obtaining relevant discovery from defendants on their infringing conduct in foreign countries, to amend this Complaint to assert claims for violations of foreign copyright laws (or laws extending similar protection) and obtaining appropriate remedies for defendants' violations of those laws.

XI. COUNT SEVEN

(Copyright Infringement – IOS Manuals)

57. Cisco alleges and incorporates by reference the allegations in paragraphs 1 through 56 above.

58. Defendants have infringed and, unless enjoined in this action, will continue to infringe Cisco's Copyrighted Works by, among other things:

- (a) Copying substantial portions of the IOS Manuals;
- (b) Distributing works containing material copied from the IOS Manuals; and
- (c) Creating derivative works based on the IOS Manuals.

59. Defendants' copying and distribution of the IOS Manuals and the creation of derivative works are not authorized by Cisco and constitute willful infringement under the Copyright Act. By reason of Defendants' acts of infringement, Cisco has suffered and will continue to suffer, unless Defendants' infringement is enjoined, irreparable injury that cannot be adequately remedied at law. Because of such willful infringement, Cisco is entitled to enhanced damages and an award of its attorneys' fees and costs pursuant to the Copyright Act.

60. Defendants' unauthorized copying and distribution of the IOS Manuals and the creation of derivative works constitute willful infringement under the copyright laws (or laws extending similar protection) of the foreign countries in which Defendants have copied, sold or distributed their infringing works. By reason of these acts of infringement, Cisco has

suffered and will continue to suffer, unless Defendants' infringement is enjoined, irreparable injury that cannot be adequately remedied at law. The exact foreign countries in which defendants have copied, sold or distributed their infringing works, and the extent of that illegal conduct, are not presently known to Cisco and can be learned only upon appropriate discovery from defendants. Cisco reserves the right, upon obtaining relevant discovery from defendants on their infringing conduct in foreign countries, to amend this Complaint to assert claims for violations of foreign copyright laws (or laws extending similar protection) and obtaining appropriate remedies for defendants' violations of those laws.

XII. COUNT EIGHT

(Trade Secret Misappropriation)

61. Cisco alleges and incorporates by reference the allegations of paragraphs 1 through 60 above.

62. Cisco maintains the source code to its IOS Software Programs as trade secrets and has taken reasonable measures to preserve the secrecy of the source code. The source code derives independent economic value from not being generally known to the public or to other persons who can obtain economic value from its disclosure or use.

63. On information and belief, Defendants have gained access to some or all of Cisco's IOS source code through improper means and/or a breach of a confidential relationship. Defendants gained such access with knowledge, or at least reason to know, that the source code is confidential to Cisco. Defendants lacked authorization to use the source code for any purpose.

64. On information and belief, Defendants misappropriated Cisco's trade secrets by making use of the IOS Software Programs source code in order to create their VRP operating system by, among other things, using the confidential source code to learn confidential information about the structure and operation of the IOS Software Programs, patterning their own development of VRP on what they learned from Cisco's confidential information, and copying portions of the source code for incorporation into the VRP operating system.

Defendants further misappropriated Cisco's trade secrets by, on information and belief, copying portions of the IOS Software Programs source code for incorporation into their VRP operating system.

65. These acts of misappropriation violate the laws of the State of Texas and the laws of other states in which acts of misappropriation have occurred. As a direct and proximate result of Defendants' misappropriation of Cisco's trade secrets, Defendants have been unjustly enriched and Cisco has sustained damages in an amount to be proved at trial. Cisco has also suffered irreparable injury as a result of Defendants' misappropriation and will continue to suffer irreparable injury that cannot be adequately remedied at law unless Defendants are enjoined from utilizing the fruits of their misappropriation or engaging in further acts of misappropriation.

66. Each of the acts of misappropriation was done willfully and maliciously by Defendants, entitling Cisco to punitive damages to be proved at trial.

67. Defendants' misappropriation of Cisco's trade secrets also constitutes violations of those laws protecting trade secrets in foreign countries in which Defendants have taken, used, disclosed or profited from Cisco's trade secrets. The identity of those foreign countries in which defendants have taken, used, disclosed or profited from Cisco's trade secrets, and the extent of such illegal conduct, are not presently known to Cisco and can be learned only through appropriate discovery from Defendants. Cisco reserves the right, upon obtaining relevant discovery from Defendants, to amend this complaint to assert claims for trade secret misappropriation and/or theft under the laws of foreign countries, and to obtain appropriate remedies for Defendants' illegal acts under the laws of foreign countries.

XIII. COUNT NINE

(Common Law Misappropriation)

68. Cisco alleges and incorporates by reference the allegations of paragraphs 1 through 67 above.

69. The CLI is a critical component of Cisco's business and represents enormous commercial value to the company. Cisco has invested substantial time and expense in the development of the CLI, a development effort that has entailed thousands of man hours of work spread over an extended period of time. Cisco also has invested substantial time and expense in training its customers on the use of the CLI.

70. By replicating the structure, organization and commands of CLI, Defendants have misappropriated the substantial commercial value of the CLI without the consent or authorization of Cisco.

71. By this misappropriation, Defendants are attempting to reap the benefits of Cisco's effort without committing the time and resources to independently develop an interface. Because they have avoided the expense of creating their own user interface, Defendants are able to price their routers at levels that would not be possible if Defendants were not obtaining a free ride on the basis of Cisco's efforts.

72. As a direct and proximate result of Defendants' misappropriation, Cisco has sustained damages in an amount to be proved at trial. Defendants' misappropriation has caused, and unless enjoined, will continue to cause, substantial competitive injury to Cisco.

XIV. COUNT TEN

(False Representation – Lanham Act § 43(a))

73. Cisco repeats and incorporates the allegations in paragraphs 1 through 72 above.

74. On information and belief, Defendants have represented to customers and prospective customers that their Quidway routers are interoperable with Cisco routers without any loss or performance, security or convenience. Such representations constitute a false and misleading characterization of the qualities and characteristics of Defendants' products in violation of Section 43(a) of the Lanham Act, 15 U.S.C. § 1125(a).

75. As a direct and proximate result of Defendants' misrepresentations of fact, Cisco has suffered and will continue to suffer irreparable injury unless Defendants are enjoined from engaging in their unlawful conduct.

76. As a direct and proximate result of Defendants' passing off, Cisco has suffered and will continue to suffer irreparable injury unless Defendants are enjoined from engaging in their unlawful conduct.

XV. COUNT ELEVEN

(Unfair Competition – Texas Common Law and Lanham Act § 44)

77. Cisco repeats and incorporates the allegations in paragraphs 1 through 76 above.

78. Defendants have engaged in unfair competition under Texas common law and under Lanham Act § 44 by, among other things, misappropriating Cisco's trade secrets, misappropriating the commercial value of the CLI, making false representations regarding the qualities and characteristics of their Quidway routers, making claims of "full intellectual property rights" under Cisco IP and mimicking Cisco's nomenclature and product numbering system to mislead customers and potential customers regarding the alleged interoperability of Quidway routers.

79. As a direct and proximate result of Defendants' acts of unfair competition, Defendants have been unjustly enriched and Cisco has sustained damages in an amount to be proved at trial. Cisco has also suffered irreparable injury as a result of Defendants' unfair competition and will continue to suffer irreparable injury unless Defendants are enjoined from utilizing the fruits of their unfair competition or engaging in further acts of unfair competition.

80. Each of the acts of unfair competition were done willfully and maliciously by Defendants, entitling Cisco to punitive damages to be proved at trial.

XVI. COUNT TWELVE

(Conversion)

81. Cisco repeats and incorporates the allegations in paragraphs 1 through 80 above.

82. On information and belief, Defendants converted Cisco's computer code by unlawfully acquiring possession of one or more computer files (i.e., one or more documents) containing Cisco's computer source code and exercising dominion and control over the computer source code in an unlawful and unauthorized manner to the exclusion of and inconsistent with Cisco's rights, tantamount to a refusal after demand.

83. As a direct and proximate result of Defendants' acts of conversion, Cisco has sustained damages in an amount to be proved at trial. Cisco has also suffered irreparable injury as a result of Defendants' conversion and will continue to suffer irreparable injury unless Defendants are enjoined from utilizing the fruits of their conversion.

84. Each of the acts of conversion were done willfully and maliciously by Defendants, entitling Cisco to punitive damages to be proved at trial.

XVII. DEMAND FOR TRIAL BY JURY

85. Cisco hereby demands a jury trial for all issues deemed to be triable by jury.

XVIII. PRAYER FOR RELIEF

WHEREFORE, Cisco respectfully requests that this Court enter judgment in its favor and against Defendants and grant the following relief:

- A. A judgment that Defendants have infringed the patents in suit.
- B. A judgment that Defendants' infringement of the patents in suit has been willful.
- C. A preliminary and permanent injunction, pursuant to 35 U.S.C. § 283, enjoining Defendants, and all persons in active concert or participation with them, from any

further acts of infringement, contributory infringement or inducement of infringement of the patents in suit.

D. An order, pursuant to 35 U.S.C. § 284, awarding Cisco damages adequate to compensate Cisco for Defendants' infringement of the patents in suit, in an amount to be determined at trial, but in no event less than a reasonable royalty.

E. An order, pursuant to 35 U.S.C. § 284, trebling all damages awarded to Cisco based on Defendants' willful infringement of the patents in suit.

F. An order, pursuant to 35 U.S.C. § 285, finding that this is an exceptional case and awarding to Cisco its reasonable attorneys fees incurred in this action.

G. A preliminary and permanent injunction enjoining Defendants, and all persons in active concert or participation with them, from infringing or contributorily infringing Cisco's copyrights in the IOS Software Programs, CLI or IOS Manuals.

H. An order requiring Defendants to account for all gains, profits and advantage derived from their infringement of Cisco's Copyrighted Works.

I. An order awarding Cisco damages against Defendants equal in amount to the damages sustained by Cisco and the profits earned by Defendants from their infringement pursuant to 17 U.S.C. § 504(b).

J. An order awarding Cisco statutory damages pursuant to 17 U.S.C. § 504(c).

K. An order awarding Cisco its attorneys fees and costs on account of Defendants' infringement pursuant to 17 U.S.C. § 505.

L. An order requiring the impoundment and destruction of all routers, computer programs and manuals, or any version or modification thereof, found to constitute an infringement of Cisco's copyrights or trade secrets.

M. A preliminary and permanent injunction enjoining Defendants, and all persons in active concert or participation with them, from misappropriating or threatening to misappropriate Cisco's trade secrets or misappropriating the commercial value of the CLI.

N. A preliminary and permanent injunction enjoining Defendants, and all persons in active concert or participation with them, from making false and misleading statements regarding the performance, characteristics or interoperability of Defendants' Quidway routers.

O. A preliminary and permanent injunction enjoining Defendants, and all persons in active concert or participation with them, from using, selling, offering for sale, marketing, distributing or placing in interstate commerce their Quidway routers, switches, or other products that use VRP, and the VRP operating system itself.

P. An order awarding Cisco damages in an amount to be determined at trial arising from Defendants' trade secret misappropriation, common law misappropriation, false and misleading representations regarding their Quidway routers, switches, or other products that use VRP, and Defendants' unfair competition.

Q. An order requiring Defendants to disgorge all ill-gotten profits earned from their unlawful conduct, together with restitution to plaintiffs arising from Defendants' unlawful conduct.

R. An order awarding Cisco the unjust enrichment gained by Defendants from their unlawful conduct.

S. An order awarding Cisco punitive damages in an amount to be determined at trial on account of Defendants' wanton, willful and malicious tortious conduct.

T. An order awarding Cisco its attorneys fees and costs in this action.

U. Such other and further relief as this Court may deem just and proper.

Dated: January 22, 2003

Respectfully submitted,

Sam Baxter

Sam F. Baxter
Attorney-In-Charge for Plaintiff
State Bar No. 01938000

McKool Smith, P.C.
P.O. Box O
505 East Travis Street, Suite 105
Marshall, TX 75670
Telephone: (903) 927-2111
Facsimile: (903) 927-2622

Jeffrey R. Bragalone
State Bar No. 02885775

McKool Smith, P.C.
300 Crescent Court, Suite 1500
Dallas, TX 75201
Telephone (214) 978-4000
Facsimile: (214)978-4044

OF COUNSEL:

ORRICK, HERRINGTON & SUTCLIFFE LLP
Chris R. Ottenweller (Ca. State Bar No. 73649)
G. Hopkins Guy (Ca. State Bar No. 124811)
1000 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 614-7400
Facsimile: (650) 614-7401

EXHIBIT A

CERTIFICATE OF REGISTRATION



OFFICIAL SEAL

This Certificate issued under the seal of the Copyright Office in accordance with title 17, United States Code, attests that registration has been made for the work identified below. The information on this certificate has been made a part of the Copyright Office records.

FORM TX
 Non-dramatic Literary Work
 UNITED STATES COPYRIGHT OFFICE

TXU 1-036-057

EFFECTIVE DATE OF REGISTRATION

JUN 14 2002

Month Day Year

REGISTER OF COPYRIGHTS
United States of America

DO NOT WRITE ABOVE THIS LINE. IF YOU NEED MORE SPACE, USE A SEPARATE CONTINUATION SHEET.

1

TITLE OF THIS WORK ▼

Cisco IOS 11.0

PREVIOUS OR ALTERNATIVE TITLES ▼ Cisco IOS Release 11.0; Cisco IOS Version 11.0; Cisco Internetwork Operating System 11.0; Cisco Internetwork Operating System Release 11.0; Cisco Internetwork Operating System Version 11.0

PUBLICATION AS A CONTRIBUTION ▼ If this work was published as a contribution to a periodical, serial, or collection, give information about the collective work in which the contribution appeared. Title of Collective Work ▼

If published in a periodical or serial give: Volume ▼ Number ▼ Issue Date ▼ On Page ▼

2NAME OF AUTHOR ▼
Cisco Systems, Inc.DATES OF BIRTH AND DEATH
Year Born ▼ Year Died ▼Was this contribution to the work a "work made for hire"? Yes NoAUTHOR'S NATIONALITY OR DOMICILE
Name of Country
OR Citizen of ▶ Domiciled in ▶ United StatesWAS THIS AUTHOR'S CONTRIBUTION TO THE WORK
Anonymous? Yes No
Pseudonymous? Yes No
If the answer to either of these questions is "Yes," see detailed instructions.**NOTE**

Under the law, the "author" of a "work made for hire" is generally the employer, not the employee (see instructions). For any part of this work that was "made for hire" check "Yes" in the space provided, give the employer (or other person for whom the work was prepared) as "Author" of that part, and leave the space for dates of birth and death blank.

NATURE OF AUTHORSHIP Briefly describe nature of material created by this author in which copyright is claimed. ▼

New and revised computer code and accompanying documentation

DATES OF BIRTH AND DEATH
Year Born ▼ Year Died ▼NAME OF AUTHOR ▼
See Attached Form TX/CON for Additional AuthorsWas this contribution to the work a "work made for hire"? Yes NoAUTHOR'S NATIONALITY OR DOMICILE
Name of Country
OR Citizen of ▶ Domiciled in ▶WAS THIS AUTHOR'S CONTRIBUTION TO THE WORK
Anonymous? Yes No
Pseudonymous? Yes No
If the answer to either of these questions is "Yes," see detailed instructions.

NATURE OF AUTHORSHIP Briefly describe nature of material created by this author in which copyright is claimed. ▼

NAME OF AUTHOR ▼

DATES OF BIRTH AND DEATH
Year Born ▼ Year Died ▼Was this contribution to the work a "work made for hire"? Yes NoAUTHOR'S NATIONALITY OR DOMICILE
Name of Country
OR Citizen of ▶ Domiciled in ▶WAS THIS AUTHOR'S CONTRIBUTION TO THE WORK
Anonymous? Yes No
Pseudonymous? Yes No
If the answer to either of these questions is "Yes," see detailed instructions.

NATURE OF AUTHORSHIP Briefly describe nature of material created by this author in which copyright is claimed. ▼

NAME OF AUTHOR ▼

DATES OF BIRTH AND DEATH
Year Born ▼ Year Died ▼Was this contribution to the work a "work made for hire"? Yes NoAUTHOR'S NATIONALITY OR DOMICILE
Name of Country
OR Citizen of ▶ Domiciled in ▶WAS THIS AUTHOR'S CONTRIBUTION TO THE WORK
Anonymous? Yes No
Pseudonymous? Yes No
If the answer to either of these questions is "Yes," see detailed instructions.

NATURE OF AUTHORSHIP Briefly describe nature of material created by this author in which copyright is claimed. ▼

YEAR IN WHICH CREATION OF THIS WORK WAS COMPLETED

This information must be given in all cases.

1995

◀ Year

DATE AND NATION OF FIRST PUBLICATION OF THIS PARTICULAR WORK

Complete this information Month ▶ Day ▶ Year ▶ Nation ▶
ONLY if this work has been published.

COPYRIGHT CLAIMANT(S) Name and address must be given even if the claimant is the same as the author given in space 2. ▼

Cisco Technology, Inc.
170 West Tasman Drive
San Jose, CA 95134

TRANSFER If the claimant(s) named here in space 4 is (are) different from the author(s) named in space 2, give a brief statement of how the claimant(s) obtained ownership of the copyright. ▼

By agreement

APPLICATION RECEIVED

JUN 14 2002

ONE DEPOSIT RECEIVED

JUN 14 2002

TWO DEPOSITS RECEIVED

FUND RECEIVED

DO NOT WRITE HERE

Page 1 of 4 pages

MORE ON BACK ▶ Complete all applicable spaces (numbers 5-8) on the reverse side of this page.
- See detailed instructions.

- Sign the form at line 8.

EXAMINED BY

FORM TX

CHECKED BY

CORRESPONDENCE
 Yes

FOR
COPYRIGHT
OFFICE
USE
ONLY

DO NOT WRITE ABOVE THIS LINE. IF YOU NEED MORE SPACE, USE A SEPARATE CONTINUATION SHEET.

PREVIOUS REGISTRATION Has registration for this work, or for an earlier version of this work, already been made in the Copyright Office?

 Yes No If your answer is "Yes," why is another registration being sought? (Check appropriate box.) ▼

- a. This is the first published edition of a work previously registered in unpublished form.
- b. This is the first application submitted by this author as copyright claimant.
- c. This is a changed version of the work, as shown by space 6 on this application.

If your answer is "Yes," give: Previous Registration Number ▶

Year of Registration ▶

5

DERIVATIVE WORK OR COMPILATION

Preexisting Material Identify any preexisting work or works that this work is based on or incorporates. ▼

Prior works by claimant and preexisting third party computer code

a 6

See instructions
before completing
this space.

Material Added to This Work Give a brief, general statement of the material that has been added to this work and in which copyright is claimed. ▼

New and revised computer code and accompanying documentation

b

DEPOSIT ACCOUNT If the registration fee is to be charged to a Deposit Account established in the Copyright Office, give name and number of Account.
Name ▶ Account Number ▶

a 7

CORRESPONDENCE Give name and address to which correspondence about this application should be sent. Name/Address/Apt/City/State/ZIP ▼

Tu T. Tsao, Esq.
 Fenwick & West LLP
 2 Palo Alto Square
 Palo Alto, CA 94306

Area code and daytime telephone number ▶ (650) 858-7696

Fax number ▶

(650) 494-1417

Email ▶ tttsao@fenwick.com

b

CERTIFICATION I, the undersigned, hereby certify that I am the

Check only one ▶

- { author
 other copyright claimant
 owner of exclusive right(s)
 authorized agent of Cisco Technology, Inc.

Name of author or other copyright claimant, or owner of exclusive right(s) ▲

of the work identified in this application and that the statements made by me in this application are correct to the best of my knowledge.

8

Typed or printed name and date ▼ If this application gives a date of publication in space 3, do not sign and submit it before that date.

Robert A. Barr, Worldwide Patent Counsel

Date ▶


 Handwritten signature of Robert A. Barr

Certificate
will be
mailed in
window
envelope
to this
address:

Name ▶ Susanne S. Morales, Paralegal / Fenwick & West LLP
 Number/Street/Apt ▶
 2 Palo Alto Square
 City/State/ZIP ▶
 Palo Alto, CA 94306

YOU MUST
 • Complete all necessary spaces
 • Sign your application in space 8
**SEND ALL ELEMENTS
IN THE SAME PACKAGE**
 1. Application form
 2. Nonrefundable filing fee in check or money order payable to Register of Copyrights
 3. Deposit material
MAIL TO
 Library of Congress
 Copyright Office
 101 Independence Avenue, S.E.
 Washington, D.C. 20559-6000
Fee
 As of July 1, 1999,
 the filing fee for Form TX is \$30.

9

*17 U.S.C. § 505(e). Any person who knowingly makes a false representation of a material fact in the application for copyright registration provided for by section 409, or in any written statement filed in connection with the application, shall be fined not more than \$2,500.
 June 1999—200,000
 WEB REV: June 1999

© 1999 GPO

U.S. GOVERNMENT PRINTING OFFICE: 1999-454-57949

CONTINUATION SHEET FOR APPLICATION FORMS

- This Continuation Sheet is used in conjunction with Forms CA, PA, SE, SR, TX, and VA, only. Indicate which basic form you are continuing in the space in the upper right-hand corner.
- If at all possible, try to fit the information called for into the spaces provided on the basic form.
- If you do not have enough space for all the information you need to give on the basic form, use this Continuation Sheet and submit it with the basic form.
- If you submit this Continuation Sheet, clip (do not tape or staple) it to the basic form and fold the two together before submitting them.
- Space A of this sheet is intended to identify the basic application. Space B is a continuation of Space 2 on the basic application. Space C is not applicable to Short forms. Space C (on the reverse side of this sheet) is for the continuation of Spaces 1, 4, or 6 on the basic application or for the continuation of Space 1 on any of the three Short Forms PA, TX, or VA.

DO NOT WRITE ABOVE THIS LINE. FOR COPYRIGHT OFFICE USE ONLY

FORM IX /CON
UNITED STATES COPYRIGHT OFFICE
TXU 1-036-057
+1A001036057

P	A	P	A	U	S	E	S	E	U	S	R	S	R	T	X	T	X	U	V	A	V	A
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

EFFECTIVE DATE OF REGISTRATION

JUN 14 2002

(Month) (Day) (Year)

CONTINUATION SHEET RECEIVED

JUN 14 2002

Page 3 of 4 pages

A
Identification
of
Application

IDENTIFICATION OF CONTINUATION SHEET: This sheet is a continuation of the application for copyright registration on the basic form submitted for the following work:

- TITLE: (Give the title as given under the heading "Title of this Work" in Space 1 of the basic form.)

Cisco IOS 11.0

- NAME(S) AND ADDRESS(ES) OF COPYRIGHT CLAIMANT(S): (Give the name and address of at least one copyright claimant as given

in Space 4 of the basic form or Space 2 of any of the Short Forms PA, TX, or VA)

Cisco Technology, Inc., 170 West Tasman Drive, San Jose, CA 95134

B
Continuation
of Space 2

NAME OF AUTHOR ▼
(See Space C)

DATES OF BIRTH AND DEATH
Year Born▼ Year Died▼

d

Was this contribution to the work AUTHOR'S NATIONALITY OR DOMICILE
a "work made for hire"? Name of Country

- Yes
 No

OR Citizen of ▶ _____
Domiciled in ▶ _____

WAS THIS AUTHOR'S CONTRIBUTION TO
THE WORK
Anonymous? Yes No
Pseudonymous? Yes No
If the answer to either
of these questions is
"Yes," see detailed
instructions.

NATURE OF AUTHORSHIP Briefly describe nature of the material created by the author in which copyright is claimed. ▼

NAME OF AUTHOR ▼

DATES OF BIRTH AND DEATH
Year Born▼ Year Died▼

e

Was this contribution to the work AUTHOR'S NATIONALITY OR DOMICILE
a "work made for hire"? Name of Country

- Yes
 No

OR Citizen of ▶ _____
Domiciled in ▶ _____

WAS THIS AUTHOR'S CONTRIBUTION TO
THE WORK
Anonymous? Yes No
Pseudonymous? Yes No
If the answer to either
of these questions is
"Yes," see detailed
instructions.

NATURE OF AUTHORSHIP Briefly describe nature of the material created by the author in which copyright is claimed. ▼

NAME OF AUTHOR ▼

DATES OF BIRTH AND DEATH
Year Born▼ Year Died▼

f

Was this contribution to the work AUTHOR'S NATIONALITY OR DOMICILE
a "work made for hire"? Name of Country

- Yes
 No

OR Citizen of ▶ _____
Domiciled in ▶ _____

WAS THIS AUTHOR'S CONTRIBUTION TO
THE WORK
Anonymous? Yes No
Pseudonymous? Yes No
If the answer to either
of these questions is
"Yes," see detailed
instructions.

NATURE OF AUTHORSHIP Briefly describe nature of the material created by the author in which copyright is claimed. ▼

Use the reverse side of this sheet if you need more space for continuation of Spaces 1, 4, or 6 of the basic form or for the

CONTINUATION OF (Check which): Space 1 Space 4 Space 6 Space 2b

Name of Author	Work for Hire	Domicile	Anonymous	Pseudo-anonymous	Nature of Contribution
ABE Staffing, Inc.	Yes	United States	Yes	No	Computer code
Metaplex, Inc.	Yes	United States	Yes	No	Computer code
Nano Solutions	Yes	United States	Yes	No	Documentation
Bev Talbott	No	United States	Yes	No	Documentation

C
Continuation
of other
Spaces

Certificate
will be
mailed in
window
envelope
to this
address:

Name ▼ Susanne S. Morales, Paralegal / Fenwick & West LLP
Number/Street/Apt ▼ 2 Palo Alto Square
City/State/ZIP ▼ Palo Alto, CA 94306

YOU MUST

- Complete all necessary spaces
- Sign your application

**SEND ALL 3 ELEMENTS
IN THE SAME PACKAGE**

1. Application form
2. Nonrefundable fee in check or money order payable to Register of Copyrights
3. Deposit Material

MAIL TO
Library of Congress, Copyright Office
101 Independence Avenue, S.E.
Washington, D.C. 20559-6000

D

Fees are effective
through January 20,
2002. After that date,
check the Copyright
Office Website at
www.loc.gov/copyright
or call (202) 707-3000 for current
fee information.

EXHIBIT B

CERTIFICATE OF REGISTRATION

OFFICIAL SEAL

This Certificate issued under the seal of the Copyright Office in accordance with title 17, United States Code, attests that registration has been made for the work identified below. The information on this certificate has been made a part of the Copyright Office records.

FORM CAFor Supplementary Registration
UNITED STATES COPYRIGHT OFFICE

REGISTRATION NUMBER

TXU 1-048-569



EFFECTIVE DATE OF SUPPLEMENTARY REGISTRATION

Aug. 20, 2002

Month Day Year

REGISTER OF COPYRIGHTS
United States of America

DO NOT WRITE ABOVE THIS LINE. IF YOU NEED MORE SPACE, USE A SEPARATE CONTINUATION SHEET.

A

Title of Work ▼

Cisco IOS 11.1

Registration Number of the Basic Registration ▼ TX 5-531-435	Year of Basic Registration ▼ 2002
Name(s) of Author(s) ▼ Cisco Systems, Inc.	Name(s) of Copyright Claimant(s) ▼ Cisco Technology, Inc.

B

Location and Nature of Incorrect Information in Basic Registration ▼

Line Number 3b Line Heading or Description

Date and Nation of First Publication of this Particular Work

Incorrect Information as It Appears in Basic Registration ▼

February 28, 1998; United States

Corrected Information ▼

N/A (please delete)

Explanation of Correction ▼

The work is unpublished.

C

Location and Nature of Information in Basic Registration to be Amplified ▼

Line Number _____ Line Heading or Description _____

Amplified Information and Explanation of Information ▼

MORE ON BACK ▶ • Complete all applicable spaces (D-G) on the reverse side of this page.
 • See detailed instructions. • Sign the form at Space F.

DO NOT WRITE HERE

Page 1 of _____ pages

FORM CA RECEIVED	FORM CA
<u>AUG 20 2002</u>	
FUNDS RECEIVED DATE	<u>AUG 20, 2002</u>
EXAMINED BY	<u>TMS</u>
CORRESPONDENCE	<input type="checkbox"/>
REFERENCE TO THIS REGISTRATION ADDED TO BASIC REGISTRATION	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO

DO NOT WRITE ABOVE THIS LINE. IF YOU NEED MORE SPACE, USE A SEPARATE CONTINUATION SHEET.

Continuation of: Part B or Part C

Line Number: 5 Line Heading or Description: Previous Registration

Incorporated Information as It Appears In Basic Registration: Box C unchecked

Corrected Information: Box C checked

Explanation of Correction: This work is a changed version.

Line Number: 2b Line Heading or Description: Name of Author

Incorrect Information as It Appears in Basic Registration: No entry

Corrected Information: See Attached Form TX/CON for Additional Authors

Explanation of Correction: Additional authors on Form TX/CON

[REDACTED] This application should be sent to [REDACTED]

To T. Tapp, Esq.

Fenwick & West LLP

**27510 Auto Square
Rancho Cucamonga, CA 91730**

Phone (650) 858-7696 Fax (650) 494-1417 Email info@newview.com

Deposit Account: If the registration fee is to be charged to a Deposit Account established in the Copyright Office, give name and number of Account.

Name _____

Account Number _____

Classification I, the undersigned, hereby certify that this work is original.

Other copyright claimant duly authorized agent of
Name of author or other copyright claimant, or owner of exclusive right(s) □

of the work identified in this application and that the statements made by me in this application are correct.

Typed or printed name: Tu T. Tsao

Handwritten signature (X) ▼

Certificate **Name:** John Doe **Date:** 10/10/2010 **Signature:** 
• Complete all necessary boxes.
• Print your signature in Space F.

Susanne S. Morales, Paralegal / Fenwick & West LLP

2. Nonresidential buildings are subject to property and payroll tax. *Applies to certain units.*

City/State/Zip ▼

101 Independence Avenue, S.E.
Washington, D.C. 20540-0001

17 U.S.C. § 506(e) Any person who knowingly makes a false representation of a material fact in the application for copyright registration provided for by section 406, or in any written statement filed in connection with the application, shall be fined not more than \$2,500.

CERTIFICATE OF REGISTRATION



This Certificate issued under the seal of the Copyright Office in accordance with title 17, United States Code, attests that registration has been made for the work identified below. The information on this certificate has been made a part of the Copyright Office records.

ORM TX
FOR A Nondramatic Literary Work
UNITED STATES COPYRIGHT OFFICE

TX 5-531-435



07080531435

EFFECTIVE DATE OF REGISTRATION

JUN 14 2002

Month Day Year

OFFICIAL SEAL

DO NOT WRITE ABOVE THIS LINE. IF YOU NEED MORE SPACE, USE A SEPARATE CONTINUATION SHEET.

TITLE OF THIS WORK ▼

1

Cisco IOS 11.1

PREVIOUS OR ALTERNATIVE TITLES ▼ Cisco IOS Release 11.1; Cisco IOS Version 11.1; Cisco Internetwork Operating System 11.1; Cisco Internetwork Operating System Release 11.1; Cisco Internetwork Operating System Version 11.1

PUBLICATION AS A CONTRIBUTION If this work was published as a contribution to a periodical, serial, or collection, give information about the collective work in which the contribution appeared. Title of Collective Work ▼

If published in a periodical or serial give: Volume ▼ Number ▼ Issue Date ▼ On Pages ▼

2NAME OF AUTHOR ▼
a Cisco Systems, Inc.

Was this contribution to the work a "work made for hire"?

Yes
 No

AUTHOR'S NATIONALITY OR DOMICILE
Name of Country
OR Citizen of ▶ _____
Domiciled in ▶ _____ United StatesDATES OF BIRTH AND DEATH
Year Born ▼ Year Died ▼WAS THIS AUTHOR'S CONTRIBUTION TO THE WORK
Anonymous? Yes No
Pseudonymous? Yes No
If the answer is either of these questions is "Yes," see detailed instructions.**NOTE**

Under the law, the "author" of a "work made for hire" is generally the employer, not the employee (see instructions). For any part of this work that was "made for hire" check "Yes" in the space provided, give the employer (or other person for whom the work was prepared) as "Author" of that part, and leave the spaces for dates of birth and death blank.

NATURE OF AUTHORSHIP Briefly describe nature of material created by this author in which copyright is claimed. ▼
New and revised computer code

NAME OF AUTHOR ▼

DATES OF BIRTH AND DEATH
Year Born ▼ Year Died ▼**b**

Was this contribution to the work a "work made for hire"?

Yes
 No

AUTHOR'S NATIONALITY OR DOMICILE
Name of Country
OR Citizen of ▶ _____
Domiciled in ▶ _____WAS THIS AUTHOR'S CONTRIBUTION TO THE WORK
Anonymous? Yes No
Pseudonymous? Yes No
If the answer is either of these questions is "Yes," see detailed instructions.**c**

Was this contribution to the work a "work made for hire"?

Yes
 No

AUTHOR'S NATIONALITY OR DOMICILE
Name of Country
OR Citizen of ▶ _____
Domiciled in ▶ _____DATES OF BIRTH AND DEATH
Year Born ▼ Year Died ▼WAS THIS AUTHOR'S CONTRIBUTION TO THE WORK
Anonymous? Yes No
Pseudonymous? Yes No
If the answer is either of these questions is "Yes," see detailed instructions.**3**YEAR IN WHICH CREATION OF THIS WORK WAS COMPLETED
a 1996 YearDATE AND NATION OF FIRST PUBLICATION OF THIS PARTICULAR WORK
b Complete this information Month ▶ FEBRUARY Day ▶ 28 Year ▶ 1996
ONLY if this work has been published. United States Nation**4**

See instructions before completing this space.

COPYRIGHT CLAIMANT(S) Name and address must be given even if the claimant is the same as the author given in space 2. ▼

Cisco Technology, Inc.
170 West Tasman Drive
San Jose, CA 95134

TRANSFER If the claimant(s) named here in space 4 is (are) different from the author(s) named in space 2, give a brief statement of how the claimant(s) obtained ownership of the copyright. ▼

By agreement

JUN 14 2002	July 16, 2002
ONE DEPOSIT RECEIVED	
JUN 14 2002	TWO DEPOSITS RECEIVED
FUND RECEIVED	

MORE ON BACK ▶ Complete all applicable spaces (numbers 5-8) on the reverse side of this page.
• See detailed instructions.DO NOT WRITE HERE
Page 1 of 4 pages

CONTINUATION SHEET FOR APPLICATION FORMS

- This Continuation Sheet is used in conjunction with Forms CA, PA, SE, SR, TX, and VA, only. Indicate which basic form you are continuing in the space in the upper right-hand corner.
- If at all possible, try to fit the information called for into the spaces provided on the basic form.
- If you do not have enough space for all the information you need to give on the basic form, use this Continuation Sheet and submit it with the basic form.
- If you submit this Continuation Sheet, clip (do not tape or staple) it to the basic form and fold the two together before submitting them.
- Space A of this sheet is intended to identify the basic application. Space B is a continuation of Space 2 on the basic application. Space C is not applicable to Short forms. Space C (on the reverse side of this sheet) is for the continuation of Spaces 1, 4, or 6 on the basic application or for the continuation of Space 1 on any of the three Short Forms PA, TX, or VA.

DO NOT WRITE ABOVE THIS LINE. FOR COPYRIGHT OFFICE USE ONLY

FORM TX /CON
UNITED STATES COPYRIGHT OFFICE

R TX 5-531-435

D10000531435

PA PAUSE SEG SEU SR SRU TX XU VA VAU

EFFECTIVE DATE OF REGISTRATION

JUN 14 2002

(Month) (Day) (Year)

CONTINUATION SHEET RECEIVED

JUN 14 2002

Page 3 of 4 pages**A**Identification
of
Application

IDENTIFICATION OF CONTINUATION SHEET: This sheet is a continuation of the application for copyright registration on the basic form submitted for the following work:

- TITLE:** (Give the title as given under the heading "Title of this Work" in Space 1 of the basic form.)

Cisco IOS 11.1

- NAME(S) AND ADDRESS(ES) OF COPYRIGHT CLAIMANT(S):** (Give the name and address of at least one copyright claimant as given in Space 4 of the basic form or Space 2 of any of the Short Forms PA, TX, or VA.)

Cisco Technology, Inc., 170 West Tasman Drive, San Jose, CA 95134

NAME OF AUTHOR ▼

(See Space C)

DATES OF BIRTH AND DEATH

Year Born▼

Year Died▼

BContinuation
of Space 2

Was this contribution to the work AUTHOR'S NATIONALITY OR DOMICILE a "work made for hire"? Name of Country

- Yes
 No

OR Citizen of ►

Domiciled in ►

WAS THIS AUTHOR'S CONTRIBUTION TO THE WORK
Anonymous? Yes No

If the answer to either of these questions is "Yes," see detailed instructions.

Pseudonymous? Yes No

NATURE OF AUTHORSHIP Briefly describe nature of the material created by the author in which copyright is claimed. ▼

NAME OF AUTHOR ▼

DATES OF BIRTH AND DEATH

Year Born▼

Year Died▼

e

Was this contribution to the work AUTHOR'S NATIONALITY OR DOMICILE a "work made for hire"? Name of Country

- Yes
 No

OR Citizen of ►

Domiciled in ►

WAS THIS AUTHOR'S CONTRIBUTION TO THE WORK
Anonymous? Yes No

If the answer to either of these questions is "Yes," see detailed instructions.

Pseudonymous? Yes No

NATURE OF AUTHORSHIP Briefly describe nature of the material created by the author in which copyright is claimed. ▼

NAME OF AUTHOR ▼

DATES OF BIRTH AND DEATH

Year Born▼

Year Died▼

f

Was this contribution to the work AUTHOR'S NATIONALITY OR DOMICILE a "work made for hire"? Name of Country

- Yes
 No

OR Citizen of ►

Domiciled in ►

WAS THIS AUTHOR'S CONTRIBUTION TO THE WORK
Anonymous? Yes No

If the answer to either of these questions is "Yes," see detailed instructions.

Pseudonymous? Yes No

NATURE OF AUTHORSHIP Briefly describe nature of the material created by the author in which copyright is claimed. ▼

Use the reverse side of this sheet if you need more space for continuation of Spaces 1, 4, or 6 of the basic form or for the continuation of Space 1 on any of the Short Forms PA, TX, or VA.

CONTINUATION OF (Check which):		<input type="checkbox"/> Space 1	<input type="checkbox"/> Space 4	<input type="checkbox"/> Space 6	<input checked="" type="checkbox"/> Space 2b	
Name of Author	Work for Hire	Domicile	Anonymous	Pseudo-anonymous	Nature of Contribution	C Continuation of other Species
Energetic Systems	Yes	United States	Yes	No	Computer code	
Metaplex, Inc.	Yes	United States	Yes	No	Computer code	
Nano Solutions	Yes	United States	Yes	No	Documentation	
Bcv Talbott	No	United States	Yes	No	Documentation	

Certificate will be mailed in window envelope to this address:

Name ▼ Susanne S. Morales, Paralegal / Fenwick & West LLP

Number/Street/Apt ▼

2 Palo Alto Square

City/State/ZIP ▼

Palo Alto, CA 94306

YOU MUST

- Complete all necessary spaces
- Sign your application

SEND ALL 3 ELEMENTS IN THE SAME PACKAGE

1. Application form
2. Nonrefundable fee in check or money order payable to Register of Copyrights
3. Deposit Material

MAIL TO

Library of Congress, Copyright Office
101 Independence Avenue, S.E.
Washington, D.C. 20559-6000

D
Fees are effective through June 30, 2002. After that date, check the Copyright Office Website at www.loc.gov/copyright/ or call (202) 707-3400 for current fee information.

EXHIBIT C

CERTIFICATE OF REGISTRATION

This Certificate issued under the seal of the Copyright Office in accordance with title 17, United States Code, attests that registration has been made for the work identified below. The information on this certificate has been made a part of the Copyright Office records.

FORM TXNondramatic Literary Work
UNITED STATES COPYRIGHT OFFICE

TXU 1-036-063



• TXU 1-036-063

EFFECTIVE DATE OF REGISTRATION

JUN 14 2002

Month Day Year

OFFICIAL SEAL**REGISTER OF COPYRIGHTS**

United States of America

DO NOT WRITE ABOVE THIS LINE. IF YOU NEED MORE SPACE, USE A SEPARATE CONTINUATION SHEET.

1**TITLE OF THIS WORK ▼**

Cisco IOS 11.2

PREVIOUS OR ALTERNATIVE TITLES ▼ Cisco IOS Release 11.2; Cisco IOS Version 11.2; Cisco Internetwork Operating System 11.2; Cisco Internetwork Operating System Release 11.2; Cisco Internetwork Operating System Version 11.2**PUBLICATION AS A CONTRIBUTION** If this work was published as a contribution to a periodical, serial, or collection, give information about the collective work in which the contribution appeared. **Title of Collective Work ▼**If published in a periodical or serial give: **Volume ▼** **Number ▼** **Issue Date ▼** **On Pages ▼****2****NAME OF AUTHOR ▼**

Cisco Systems, Inc.

DATES OF BIRTH AND DEATH
Year Born ▼ Year Died ▼Was this contribution to the work a "work made for hire"?
 Yes
 No
 AUTHOR'S NATIONALITY OR DOMICILE
Name of Country
OR Citizen of ▶ _____
Domiciled in ▶ _____ United States**WAS THIS AUTHOR'S CONTRIBUTION TO THE WORK**
Anonymous? Yes No
Pseudonymous? Yes No
If the answer to either of these questions is "Yes," see detailed instructions.**NOTE**

Under the law, the "author" of a "work made for hire" is generally the employer, not the employee (see instructions). For any part of this work that was "made for hire" check "Yes" in the space provided, give the employer (or other person for whom the work was prepared) as "Author" of that part, and leave the space for dates of birth and death blank.

b **NAME OF AUTHOR ▼**

See Attached Form TX/CON for Additional Authors

DATES OF BIRTH AND DEATH
Year Born ▼ Year Died ▼Was this contribution to the work a "work made for hire"?
 Yes
 No
 AUTHOR'S NATIONALITY OR DOMICILE
Name of Country
OR Citizen of ▶ _____
Domiciled in ▶ _____**WAS THIS AUTHOR'S CONTRIBUTION TO THE WORK**
Anonymous? Yes No
Pseudonymous? Yes No
If the answer to either of these questions is "Yes," see detailed instructions.**c** **NATURE OF AUTHORSHIP** Briefly describe nature of material created by this author in which copyright is claimed. ▼**NAME OF AUTHOR ▼****DATES OF BIRTH AND DEATH**
Year Born ▼ Year Died ▼Was this contribution to the work a "work made for hire"?
 Yes
 No
 AUTHOR'S NATIONALITY OR DOMICILE
Name of Country
OR Citizen of ▶ _____
Domiciled in ▶ _____**WAS THIS AUTHOR'S CONTRIBUTION TO THE WORK**
Anonymous? Yes No
Pseudonymous? Yes No
If the answer to either of these questions is "Yes," see detailed instructions.**NATURE OF AUTHORSHIP** Briefly describe nature of material created by this author in which copyright is claimed. ▼**3****a** **YEAR IN WHICH CREATION OF THIS WORK WAS COMPLETED** This information must be given in all cases.
1996 ▶ Year**b** **DATE AND NATION OF FIRST PUBLICATION OF THIS PARTICULAR WORK**

Complete this information Month ▶ _____ Day ▶ _____ Year ▶ _____ Nation ▶ _____

4

See instructions before completing this space.

COPYRIGHT CLAIMANT(S) Name and address must be given even if the claimant is the same as the author given in space 2. ▼Cisco Technology, Inc.
170 West Tasman Drive
San Jose, CA 95134**APPLICATION RECEIVED**

JUN 14 2002

ONE DEPOSIT RECEIVED

JUN 14 2002

TWO DEPOSITS RECEIVED

FUND'S RECEIVED

DO NOT WRITE HERE
OR FEE USE ONLY**MORE ON BACK ▶** • Complete all applicable spaces (numbers 5-9) on the reverse side of this page.

• See detailed instructions.

• Sign the form at line 8.

DO NOT WRITE HERE

Page 1 of 4 pages

EXAMINED BY	FORM TX
TMS	
CHECKED BY	
<input type="checkbox"/> CORRESPONDENCE	FOR
<input checked="" type="checkbox"/> Yes	COPYRIGHT
	OFFICE
	USE
	ONLY

DO NOT WRITE ABOVE THIS LINE. IF YOU NEED MORE SPACE, USE A SEPARATE CONTINUATION SHEET.

PREVIOUS REGISTRATION Has registration for this work, or for an earlier version of this work, already been made in the Copyright Office?

- Yes No If your answer is "Yes," why is another registration being sought? (Check appropriate box.) ▼
 a. This is the first published edition of a work previously registered in unpublished form.
 b. This is the first application submitted by this author as copyright claimant.
 c. This is a changed version of the work, as shown by space 6 on this application.

If your answer is "Yes," give: Previous Registration Number ▶

Pending

Year of Registration ▶

2002

5

DERIVATIVE WORK OR COMPILATION

Preexisting Material Identify any preexisting work or works that this work is based on or incorporates. ▼

Prior works by claimant and preexisting third party computer code

a
6

See instructions
before completing
this space.

Material Added to This Work Give a brief, general statement of the material that has been added to this work and in which copyright is claimed. ▼
 New and revised computer code and accompanying documentation

b

DEPOSIT ACCOUNT If the registration fee is to be charged to a Deposit Account established in the Copyright Office, give name and number of Account.
 Name ▼ Account Number ▼

a
7

CORRESPONDENCE Give name and address to which correspondence about this application should be sent. Name/Address/Apt/City/State/ZIP ▼

b

Tu T. Tsao, Esq.
 Fenwick & West LLP
 2 Palo Alto Square
 Palo Alto, CA 94306

Area code and daytime telephone number ▶ (650) 858-7696

Fax number ▶

(650) 494-1417

Email ▶ tttsao@fenwick.com

CERTIFICATION I, the undersigned, hereby certify that I am the

Check only one ▶

- author
 other copyright claimant
 owner of exclusive right(s)
 authorized agent of Cisco Technology, Inc.

Name of author or other copyright claimant, or owner of exclusive right(s) ▲

of the work identified in this application and that the statements made by me in this application are correct to the best of my knowledge.

8

Typed or printed name and date ▼ If this application gives a date of publication in space 3, do not sign and submit it before that date.

Robert A. Barr, Worldwide Patent Counsel

Date ▶

Handwritten signature □ ▼
 X — Fenwick —

Certificate
will be
mailed in
window
envelope
to this
address:

Name ▼ Susanne S. Morales, Paralegal / Fenwick & West LLP
 Number/Street/Apt ▼
 2 Palo Alto Square
 City/State/ZIP ▼
 Palo Alto, CA 94306

YOU MUST
 • Complete all necessary spaces
 • Sign your application in space 3
 SEND ALL ELEMENTS
 IN THE SAME PACKAGE
 1. Application form
 2. Nonrefundable filing fee in check or money order As of
 payable to Register of Copyrights July 1,
 3. Deposit material 1999.
 MAIL TO
 Library of Congress
 Copyright Office
 101 Independence Avenue, S.E.
 Washington, D.C. 20559-6000
 Filing
 fee for
 Form TX
 is \$30.

CONTINUATION SHEET FOR APPLICATION FORMS

- This Continuation Sheet is used in conjunction with Forms CA, PA, SE, SR, TX, and VA, only. Indicate which basic form you are continuing in the space in the upper right-hand corner.
- If at all possible, try to fit the information called for into the spaces provided on the basic form.
- If you do not have enough space for all the information you need to give on the basic form, use this Continuation Sheet and submit it with the basic form.
- If you submit this Continuation Sheet, clip (do not tape or staple) it to the basic form and fold the two together before submitting them.
- Space A of this sheet is intended to identify the basic application. Space B is a continuation of Space 2 on the basic application. Space B is not applicable to Short forms. Space C (on the reverse side of this sheet) is for the continuation of Spaces 1, 4, or 6 on the basic application or for the continuation of Space 1 on any of the three Short Forms PA, TX, or VA.

DO NOT WRITE ABOVE THIS LINE. FOR COPYRIGHT OFFICE USE ONLY

FORM TX /CON
UNITED STATES COPYRIGHT OFFICE
TXU 1-036-063
17 SEP 10 2002

PA	PAUSE	SEG	SEU	SR	SRU	TX	TXU	VA	VAU
----	-------	-----	-----	----	-----	----	-----	----	-----

EFFECTIVE DATE OF REGISTRATION

JUN 1 4 2002

(Month) (Day) (Year)

CONTINUATION SHEET RECEIVED

JUN 1 4 2002

Page 3 of 4 pages**A**Identification
of
Application

IDENTIFICATION OF CONTINUATION SHEET: This sheet is a continuation of the application for copyright registration on the basic form submitted for the following work:

- TITLE:** (Give the title as given under the heading "Title of this Work" in Space 1 of the basic form.)
Cisco IOS 11.2

- NAME(S) AND ADDRESS(ES) OF COPYRIGHT CLAIMANT(S):** (Give the name and address of at least one copyright claimant as given in Space 4 of the basic form or Space 2 of any of the Short Forms PA, TX, or VA)
Cisco Technology, Inc., 170 West Tasman Drive, San Jose, CA 95134

BContinuation
of Space 2
NAME OF AUTHOR ▼
(See Space C)

DATES OF BIRTH AND DEATH
Year Born▼ Year Died▼

Was this contribution to the work **AUTHOR'S NATIONALITY OR DOMICILE**
a "work made for hire"? Name of Country

- Yes
 No

OR Citizen of ► _____
Domiciled in ► _____

**WAS THIS AUTHOR'S CONTRIBUTION TO
THE WORK**
Anonymous? Yes No If the answer to either
of these questions is
"Yes," see detailed
instructions.
Pseudonymous? Yes No

NATURE OF AUTHORSHIP Briefly describe nature of the material created by the author in which copyright is claimed. ▼

NAME OF AUTHOR ▼
DATES OF BIRTH AND DEATH
Year Born▼ Year Died▼
e

Was this contribution to the work **AUTHOR'S NATIONALITY OR DOMICILE**
a "work made for hire"? Name of Country

- Yes
 No

OR Citizen of ► _____
Domiciled in ► _____

**WAS THIS AUTHOR'S CONTRIBUTION TO
THE WORK**
Anonymous? Yes No If the answer to either
of these questions is
"Yes," see detailed
instructions.
Pseudonymous? Yes No

NATURE OF AUTHORSHIP Briefly describe nature of the material created by the author in which copyright is claimed. ▼

NAME OF AUTHOR ▼
DATES OF BIRTH AND DEATH
Year Born▼ Year Died▼
f

Was this contribution to the work **AUTHOR'S NATIONALITY OR DOMICILE**
a "work made for hire"? Name of Country

- Yes
 No

OR Citizen of ► _____
Domiciled in ► _____

**WAS THIS AUTHOR'S CONTRIBUTION TO
THE WORK**
Anonymous? Yes No If the answer to either
of these questions is
"Yes," see detailed
instructions.
Pseudonymous? Yes No

NATURE OF AUTHORSHIP Briefly describe nature of the material created by the author in which copyright is claimed. ▼

C

CONTINUATION OF (Check which):		<input type="checkbox"/> Space 1	<input type="checkbox"/> Space 4	<input type="checkbox"/> Space 6	<input checked="" type="checkbox"/> Space 4b	Nature of Contribution	Continuation of other Spaces
Name of Author	Work for Hire	Domicile	Anonymous	Pseudo-nymous			
ABE Staffing Services, Inc.	Yes	United States	Yes	No	Computer code		
HCL America, Inc.	Yes	United States	Yes	No	Computer code		
HCL Consulting Limited	Yes	India	Yes	No	Computer code		
Network Aware, Inc.	Yes	United States	Yes	No	Computer code		
Metaplex, Inc.	Yes	United States	Yes	No	Documentation		
Nano Solutions	Yes	United States	Yes	No	Documentation		
NSA	Yes	United States	Yes	No	Documentation		
Oakhill Publications/ Computer Education Consulting	Yes	United States	Yes	No	Documentation		
Rick Barron	No	United States	Yes	No	Documentation		
Bev Talbott	No	United States	Yes	No	Documentation		

Certificate
will be
mailed in
window
envelope
to this
address:

Name ▼
Susanne S. Morales, Paralegal / Fenwick & West LLP

Number/Street/Apt ▼

2 Palo Alto Square

City/State/ZIP ▼

Palo Alto, CA 94306

YOU MUST
• Complete all necessary spaces
• Sign your application

**SEND ALL ELEMENTS
IN THE SAME PACKAGE**

1. Application form
2. Nonrefundable fee in check or money order payable to Register of Copyrights
3. Deposit Material

MAIL TO
Library of Congress, Copyright Office
101 Independence Avenue, S.E.
Washington, D.C. 20559-6000

D

Fees are effective
through June 30,
2002. After that date,
check the Copyright
Office Website at
www.loc.gov/copyright
or call (202) 707-3000 for current
fee information.

EXHIBIT D

Copyright fees are subject to change.
For current fees, check the Copyright Office website at www.copyright.gov, write the Copyright Office, or call (202) 707-3000.

FORM CA

For Supplementary Registration
UNITED STATES COPYRIGHT OFFICE
REGISTRATION NUMBER _____

TX	TXU	PA	PAU	VA	VAU	SR	SRU	RE
----	-----	----	-----	----	-----	----	-----	----

EFFECTIVE DATE OF SUPPLEMENTARY REGISTRATION

Month Day Year

DO NOT WRITE ABOVE THIS LINE. IF YOU NEED MORE SPACE, USE A SEPARATE CONTINUATION SHEET.

A**Title of Work ▼****Cisco IOS 11.3****Registration Number of the Basic Registration ▼****TXu 1-036-082****Year of Basic Registration ▼****2002****Name(s) of Author(s) ▼****Please see Space D for list of author names****Name(s) of Copyright Claimant(s) ▼****Cisco Technology, Inc.****B****Location and Nature of Incorrect Information in Basic Registration ▼**

Line Number	2a	Line Heading or Description	Name of Author
--------------------	-----------	------------------------------------	-----------------------

Incorrect Information as It Appears in Basic Registration ▼**Cisco Systems, Inc.****Corrected Information ▼****Cisco Systems Sales & Services, Inc.****Explanation of Correction ▼****correct name of author****C****Location and Nature of Information in Basic Registration to be Amplified ▼**

Line Number	2b and C	Line Heading or Description	Name of Author
--------------------	-----------------	------------------------------------	-----------------------

Amplified Information and Explanation of Information ▼**Please add to the following to the list of authors:****Name of Author: Cisco Technology, Inc.****Work for Hire: Yes****Domicile: United States****Anonymous: No****Pseudonymous: No****Nature of Contribution: Computer code and documentation****MORE ON BACK ►**

- Complete all applicable spaces (D-G) on the reverse side of this page.
- See detailed instructions.
- Sign the form at Space F.

DO NOT WRITE HERE

Page 1 of _____ pages

FUNDS RECEIVED DATE

EXAMINED BY

CORRESPONDENCE □

**REFERENCE TO THIS REGISTRATION ADDED TO
BASIC REGISTRATION** YES NO

**FOR
COPYRIGHT
OFFICE
USE
ONLY****DO NOT WRITE ABOVE THIS LINE. IF YOU NEED MORE SPACE, USE A SEPARATE CONTINUATION SHEET.**Continuation of: Part B or Part C Part A

Cisco Systems, Inc.
 HCL America, Inc.
 HCL Consulting Limited
 Metaplex, Inc.
 Technosoft Corp.
 Nano Solutions
 Oakhill Publications / Computer Education Consulting
 ABE Staffing Services, Inc.
 Lasselle-Ramsay
 Kevin Shafer
 Rick Barron

D**Correspondence:** Give name and address to which correspondence about this application should be sent.

Tu T. Tsao, Esq.
 Fenwick & West LLP
 801 California Street
 Mountain View, CA 94041

Phone (650) 335-7696

Fax (650) 938-5200

Email ttsao@fenwick.com**E****Deposit Account:** If the registration fee is to be charged to a Deposit Account established in the Copyright Office, give name and number of Account.

Name _____

Account Number _____

Certification: I, the undersigned, hereby certify that I am the: (Check only one)

author owner of exclusive right(s)
 other copyright claimant duly authorized agent of **Cisco Technology, Inc.**

Name of author or other copyright claimant, or owner of exclusive right(s) ▲

of the work identified in this application and that the statements made by me in this application are correct to the best of my knowledge.

Typed or printed name ▼

Robert A. Barr, Worldwide Patent Counsel

Date ▼

1/8/03

Handwritten signature (X) ▼

**Certificate
will be
mailed in
window
envelope
to this
address:**

Name ▼
Susanne S. Morales, Paralegal / Fenwick & West LLP
 Number/Street/Apt ▼
801 California Street
 City/State/ZIP ▼
Mountain View, CA 94041

YOU MUST
 • Complete all necessary spaces.
 • Sign your application in Space F.
**SEND ALL INFORMATION
PRINTED, SIGNED, AND
MAILED.**
 1. Application form
 2. Nonrefundable filing fee in check or
 money order payable to Register of
 Copyrights
MAIL TO
 Library of Congress
 Copyright Office
 101 Independence Avenue, S.E.
 Washington, D.C. 20559-6000

Fees are subject to
 change. For current
 fees, check the
 Copyright Office
 website at
www.copyright.gov,
 or call the Copyright
 Office, or write:
 (202) 707-3000.

G

*17 U.S.C. § 506(e): Any person who knowingly makes a false representation of a material fact in the application for copyright registration provided for by section 409, or in any written statement filed in connection with the application, shall be fined not more than \$2,500.

CERTIFICATE OF REGISTRATION

This Certificate issued under the seal of the Copyright Office in accordance with title 17, United States Code, attests that registration has been made for the work identified below. The information on this certificate has been made a part of the Copyright Office records.

FORM TX
For Dramatic Literary Work
UNITED STATES COPYRIGHT OFFICE

TXU 1-036-062



EFFECTIVE DATE OF REGISTRATION

JUN 14 2002

Month Day Year

OFFICIAL SEAL

REGISTER OF COPYRIGHTS

United States of America

DO NOT WRITE ABOVE THIS LINE. IF YOU NEED MORE SPACE, USE A SEPARATE CONTINUATION SHEET.

1

TITLE OF THIS WORK ▼

Cisco IOS 11.3

PREVIOUS OR ALTERNATIVE TITLES ▼ Cisco IOS Release 11.3; Cisco IOS Version 11.3; Cisco Internetwork Operating System 11.3; Cisco Internetwork Operating System Release 11.3; Cisco Internetwork Operating System Version 11.3

PUBLICATION AS A CONTRIBUTION If this work was published as a contribution to a periodical, serial, or collection, give information about the collective work in which the contribution appeared. Title of Collective Work ▼

If published in a periodical or serial give: Volume ▼ Number ▼ Issue Date ▼ On Page ▼

2

a NAME OF AUTHOR ▼
Cisco Systems, Inc.

Was this contribution to the work a "work made for hire"?

 Yes No

AUTHOR'S NATIONALITY OR DOMICILE

Name of Country

OR { Citizen of ▶

Domiciled in ▶ United States

DATES OF BIRTH AND DEATH

Year Born ▼ Year Died ▼

WAS THIS AUTHOR'S CONTRIBUTION TO THE WORK
Anonymous? Yes No
Pseudonymous? Yes No
If the answer to either of these questions is "Yes," see detailed instructions.

NOTE

Under the law, the "author" of a "work made for hire" is generally the employer, not the employee (see instructions). For any part of this work that was "made for hire" check "Yes" in the space provided, give the employer (or other person for whom the work was prepared) as "Author" of that part, and leave the space for dates of birth and death blank.

NATURE OF AUTHORSHIP Briefly describe nature of material created by this author in which copyright is claimed. ▼
New and revised computer code and accompanying documentationDATES OF BIRTH AND DEATH
Year Born ▼ Year Died ▼b NAME OF AUTHOR ▼
See Attached Form TX/CON for Additional Authors

Was this contribution to the work a "work made for hire"?

 Yes No

AUTHOR'S NATIONALITY OR DOMICILE

Name of Country

OR { Citizen of ▶

Domiciled in ▶

WAS THIS AUTHOR'S CONTRIBUTION TO THE WORK
Anonymous? Yes No
Pseudonymous? Yes No
If the answer to either of these questions is "Yes," see detailed instructions.

NATURE OF AUTHORSHIP Briefly describe nature of material created by this author in which copyright is claimed. ▼

c NAME OF AUTHOR ▼

DATES OF BIRTH AND DEATH
Year Born ▼ Year Died ▼

Was this contribution to the work a "work made for hire"?

 Yes No

AUTHOR'S NATIONALITY OR DOMICILE

Name of Country

OR { Citizen of ▶

Domiciled in ▶

WAS THIS AUTHOR'S CONTRIBUTION TO THE WORK
Anonymous? Yes No
Pseudonymous? Yes No
If the answer to either of these questions is "Yes," see detailed instructions.

NATURE OF AUTHORSHIP Briefly describe nature of material created by this author in which copyright is claimed. ▼

3 a YEAR IN WHICH CREATION OF THIS WORK WAS COMPLETED
1997 ◀ Year in all cases.

b DATE AND NATION OF FIRST PUBLICATION OF THIS PARTICULAR WORK

Complete this information Month ▶ Day ▶ Year ▶ Nation ▶

4
See instructions before completing this space.

COPYRIGHT CLAIMANT(S) Name and address must be given even if the claimant is the same as the author given in space 2. ▼

Cisco Technology, Inc.
170 West Tasman Drive
San Jose, CA 95134

TRANSFER If the claimant(s) named here in space 4 is (are) different from the author(s) named in space 2, give a brief statement of how the claimant(s) obtained ownership of the copyright. ▼

By agreement

DO NOT WRITE HERE
OFFICE USE ONLYAPPLICATION RECEIVED
JUN 14 2002ONE DEPOSIT RECEIVED
JUN 14 2002

TWO DEPOSITS RECEIVED

FUNDS RECEIVED

MORE ON BACK ▶ • Complete all applicable spaces (numbers 6-9) on the reverse side of this page.
• See detailed instructions.
• Sign the form at line 6.DO NOT WRITE HERE
Page 1 of 4 pages

EXAMINED BY	<i>TMS</i>	FORM TX
CHECKED BY		
<input type="checkbox"/> CORRESPONDENCE		
<input checked="" type="checkbox"/> Yes		
FOR COPYRIGHT OFFICE USE ONLY		

DO NOT WRITE ABOVE THIS LINE. IF YOU NEED MORE SPACE, USE A SEPARATE CONTINUATION SHEET.

PREVIOUS REGISTRATION Has registration for this work, or for an earlier version of this work, already been made in the Copyright Office?

Yes No If your answer is "Yes," why is another registration being sought? (Check appropriate box.) ▼

- a. This is the first published edition of a work previously registered in unpublished form.
- b. This is the first application submitted by this author as copyright claimant.
- c. This is a changed version of the work, as shown by space 6 on this application.

If your answer is "Yes," give Previous Registration Number ▶

Pending

Year of Registration ▶

2002

5

DERIVATIVE WORK OR COMPILED

Preexisting Material Identify any preexisting work or works that this work is based on or incorporates. ▼

Prior works by claimant and preexisting third party computer code

a 6

See instructions
before completing
this space.

Material Added to This Work Give a brief, general statement of the material that has been added to this work and in which copyright is claimed. ▼
New and revised computer code and accompanying documentation

b

DEPOSIT ACCOUNT If the registration fee is to be charged to a Deposit Account established in the Copyright Office, give name and number of Account.
Name ▼ Account Number ▼

a 7

7

CORRESPONDENCE Give name and address to which correspondence about this application should be sent. Name/Address/Apt/City/State/ZIP ▼
Tu T. Tsao, Esq.
Fenwick & West LLP
2 Palo Alto Square
Palo Alto, CA 94306

b

8

Area code and daytime telephone number ▶ (650) 858-7696

Fax number ▶

(650) 494-1417

Email ▶ tttsao@fenwick.com

CERTIFICATION* I, the undersigned, hereby certify that I am the

Check only one ▶

{ author
 other copyright claimant
 owner of exclusive right(s)
 authorized agent of Cisco Technology, Inc.

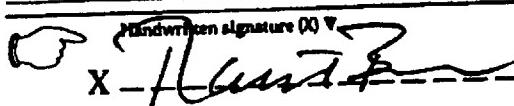
Name of author or other copyright claimant, or owner of exclusive right(s) ▲

of the work identified in this application and that the statements made
by me in this application are correct to the best of my knowledge.

Typed or printed name and date ▼ If this application gives a date of publication in space 3, do not sign and submit it before that date.

Robert A. Barr, Worldwide Patent Counsel

Date ▶


Handwritten signature □ ▼
X - Robert Barr

Certificate
will be
mailed in
window
envelope
to this
address:

Name ▼
Susanne S. Morales, Paralegal / Fenwick & West LLP
Number/Street/Apt ▼
2 Palo Alto Square
City/State/ZIP ▼
Palo Alto, CA 94306

YOU MUST
• Complete all necessary spaces
• Sign your application in space 6
SEND ALL ELEMENTS
IN THE SAME PACKAGE
1. Application form
2. Nonrefundable filing fee in check or money order As of
payable to Register of Copyrights July 1,
3. Deposit material 1999,
MAIL TO the
Library of Congress
Copyright Office
101 Independence Avenue, S.E.
Washington, D.C. 20559-6000
the
filing
fee for
Form TX
is \$30.

9

*17 U.S.C. § 506(e) Any person who knowingly makes a false representation of a material fact in the application for copyright registration provided for by section 408, or in any written statement filed in connection
with the application, shall be fined not more than \$2,500.
June 1999 - 200,000
WEB REV: June 1999

www.copyright.gov

U.S. GOVERNMENT PRINTING OFFICE: 1999-454-87849

CONTINUATION SHEET FOR APPLICATION FORMS

FORM TX /CON
UNITED STATES COPYRIGHT OFFICE

TXU 1-036-062

07/01/0362

P	A	P	A	S	E	G	S	E	S	R	S	R	T	X	T	X	U	V	A	V	A
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

EFFECTIVE DATE OF REGISTRATION

JUN 14 2002

(Month) (Day) (Year)

CONTINUATION SHEET RECEIVED

JUN 14 2002

Page 3 of 4 pages

DO NOT WRITE ABOVE THIS LINE. FOR COPYRIGHT OFFICE USE ONLY

IDENTIFICATION OF CONTINUATION SHEET: This sheet is a continuation of the application for copyright registration on the basic form submitted for the following work:

- **TITLE:** (Give the title as given under the heading "Title of this Work" in Space 1 of the basic form.)

Cisco IOS 11.3

- **NAME(S) AND ADDRESS(ES) OF COPYRIGHT CLAIMANT(S):** (Give the name and address of at least one copyright claimant as given in Space 4 of the basic form or Space 2 of any of the Short Forms PA, TX, or VA.)
Cisco Technology, Inc., 170 West Tasman Drive, San Jose, CA 95134

A
Identification of ApplicationNAME OF AUTHOR ▼
(See Space C)DATES OF BIRTH AND DEATH
Year Born▼ Year Died▼**d**Was this contribution to the work AUTHOR'S NATIONALITY OR DOMICILE
a "work made for hire"? Name of Country

- Yes
 No

OR Citizen of ► _____
Domiciled in ► _____WAS THIS AUTHOR'S CONTRIBUTION TO
THE WORK
Anonymous? Yes No If the answer to either
of these questions is
"Yes," see detailed
instructions.
Pseudonymous? Yes No**B**
Continuation of Space 2

NATURE OF AUTHORSHIP Briefly describe nature of the material created by the author in which copyright is claimed. ▼

NAME OF AUTHOR ▼

DATES OF BIRTH AND DEATH
Year Born▼ Year Died▼**e**Was this contribution to the work AUTHOR'S NATIONALITY OR DOMICILE
a "work made for hire"? Name of Country

- Yes
 No

OR Citizen of ► _____
Domiciled in ► _____WAS THIS AUTHOR'S CONTRIBUTION TO
THE WORK
Anonymous? Yes No If the answer to either
of these questions is
"Yes," see detailed
instructions.
Pseudonymous? Yes No

NATURE OF AUTHORSHIP Briefly describe nature of the material created by the author in which copyright is claimed. ▼

NAME OF AUTHOR ▼

DATES OF BIRTH AND DEATH
Year Born▼ Year Died▼**f**Was this contribution to the work AUTHOR'S NATIONALITY OR DOMICILE
a "work made for hire"? Name of Country

- Yes
 No

OR Citizen of ► _____
Domiciled in ► _____WAS THIS AUTHOR'S CONTRIBUTION TO
THE WORK
Anonymous? Yes No If the answer to either
of these questions is
"Yes," see detailed
instructions.
Pseudonymous? Yes No

NATURE OF AUTHORSHIP Briefly describe nature of the material created by the author in which copyright is claimed. ▼

Use the reverse side of this sheet if you need more space for continuation of Spaces 1, 4, or 6 of the basic form or for the
continuation of Space 1 on any of the Short Forms PA, TX, or VA.

CONTINUATION OF (Check which):		<input type="checkbox"/> Space 1	<input type="checkbox"/> Space 4	<input type="checkbox"/> Space 6	<input checked="" type="checkbox"/> Space 9	
Name of Author	Work for Hire	Domicile	Anonymous	Pseudonymous	Nature of Contribution	
HCL America, Inc.	Yes	United States	Yes	No	Computer code	Continuation of other Spaces
HCL Consulting Limited	Yes	India	Yes	No	Computer code	
Metaplex, Inc.	Yes	United States	Yes	No	Computer code	
Technosoft Corp.	Yes	United States	Yes	No	Computer code	
Nano Solutions	Yes	United States	Yes	No	Documentation	
Oakhill Publications/ Computer Education Consulting	Yes	United States	Yes	No	Documentation	
ABE Staffing Services, Inc.	Yes	United States	Yes	No	Documentation	
Lasselle-Ramsay	Yes	United States	Yes	No	Documentation	
Kevin Shafer	No	United States	Yes	No	Documentation	
Rick Barron	No	United States	Yes	No	Documentation	

Certificate
will be
mailed in
window
envelope
to this
address:

Name ▼
Susanne S. Morales, Paralegal / Fenwick & West LLP

Number/Street/Apt ▼

2 Palo Alto Square

City/State/ZIP ▼

Palo Alto, CA 94306

YOU MUST
• Complete all necessary spaces
• Sign your application

**SEND ALL ELEMENTS
IN THE SAME PACKAGE**

1. Application form
2. Nonrefundable fee in check or money order payable to Register of Copyrights
3. Deposit Material

MAIL TO
Library of Congress, Copyright Office
101 Independence Avenue, S.E.
Washington, D.C. 20559-6000

C

Continuation
of other
Spaces

D

Fees are effective
through June 26,
2002. After that date,
check the Copyright
Office Website at
www.loc.gov/copyright/
or call (202)
707-3000 for current
fee information.

EXHIBIT E

TX TXU PA PAU VA VAU SR SRU RE
EFFECTIVE DATE OF SUPPLEMENTARY REGISTRATION

Month Day Year

DO NOT WRITE ABOVE THIS LINE. IF YOU NEED MORE SPACE, USE A SEPARATE CONTINUATION SHEET.

A

Title of Work ▼

Cisco IOS 12.0

Registration Number of the Basic Registration ▼

TXU 1-036-064

Year of Basic Registration ▼

2002

Name(s) of Author(s) ▼

Please see Space D for list of author names

Name(s) of Copyright Claimant(s) ▼

Cisco Technology, Inc.

B

Location and Nature of Incorrect Information in Basic Registration ▼

Line Number 2a Line Heading or Description Name of Author

Incorrect Information as It Appears in Basic Registration ▼

Cisco Systems, Inc.

Corrected Information ▼

Cisco Systems Sales & Services, Inc.

Explanation of Correction ▼

correct name of author

C

Location and Nature of Information in Basic Registration to be Amplified ▼

Line Number 2b and C Line Heading or Description Name of Author

Amplified Information and Explanation of Information ▼

Please add the following to the list of authors:

Name of Author: Cisco Technology, Inc.

Work for Hire: Yes

Domicile: United States

Anonymous: No

Pseudonymous: No

Nature of Contribution: Computer code and documentation

MORE ON BACK ►

- Complete all applicable spaces (D-G) on the reverse side of this page.
- See detailed instructions.
- Sign the form at Space F.

DO NOT WRITE HERE

Page 1 of _____ pages

FUND'S RECEIVED DATE

EXAMINED BY

CORRESPONDENCE

REFERENCE TO THIS REGISTRATION ADDED TO
BASIC REGISTRATION YES NO

FOR
COPYRIGHT
OFFICE
USE
ONLY**DO NOT WRITE ABOVE THIS LINE. IF YOU NEED MORE SPACE, USE A SEPARATE CONTINUATION SHEET.**Continuation of: Part B or Part C Part A

Cisco Systems, Inc.
 Adecco Employment Services
 Avnisoft Corporation
 HCL Consulting Limited
 HCL America, Inc.
 H.L. Yoh Company LLC
 Aquas
 Metaplex, Inc.
 Rapidigm
 Wipro Limited
 Lasselle-Ramsay
 Oakhill Publications / Computer Education Consulting
 Rick Barron
 On-Call Consultants, Inc.
 Judy Melanson

Correspondence: Give name and address to which correspondence about this application should be sent.

Tu T. Tsao, Esq.
 Fenwick & West LLP
 801 California Street
 Mountain View, CA 94041

Phone (650) 335-7696

Fax (650) 938-5200

Email ttsaoo@fenwick.com

Deposit Account: If the registration fee is to be charged to a Deposit Account established in the Copyright Office, give name and number of Account.

Name _____

Account Number _____

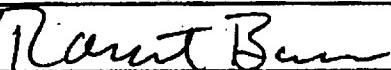
Certification: I, the undersigned, hereby certify that I am the: (Check only one)

author owner of exclusive right(s)
 other copyright claimant duly authorized agent of **Cisco Technology, Inc.**

Name of author or other copyright claimant, or owner of exclusive right(s) ▲

of the work identified in this application and that the statements made by me in this application are correct to the best of my knowledge.

Typed or printed name ▼ Robert A. Barr, Worldwide Patent Counsel

Date ▼ **1/8/03**Handwritten signature (X) ▼ 

Certificate
 will be
 mailed in
 window
 envelope
 to this
 address:

Name ▼
Susanne S. Morales, Paralegal / Fenwick & West LLP

Number/Street/Apt ▼

801 California Street

City/State/ZIP ▼

Mountain View, CA 94041

YOU MUST:
 • Complete all necessary spaces.
 • Sign your application in Space F

**SEND ALL DOCUMENTS
 ON ONE PAGE**

1. Application form
2. Nonrefundable filing fee in check or money order payable to Register of Copyrights

MAIL TO:

Library of Congress
 Copyright Office
 101 Independence Avenue, S.E.
 Washington, D.C. 20559-6000

Fees are subject to
 change. For current
 fees, see
 Circular 500,
 available at
www.copyright.gov,
 or the Copyright
 Office, or call
 (202) 707-3000.

*17 U.S.C. § 506(e): Any person who knowingly makes a false representation of a material fact in the application for copyright registration provided for by section 406, or in any written statement filed in connection with the application, shall be fined not more than \$2,500.

CERTIFICATE OF REGISTRATION



This Certificate issued under the seal of the Copyright Office in accordance with title 17, United States Code, attests that registration has been made for the work identified below. The information on this certificate has been made a part of the Copyright Office records.

FORM TX
a Non-dramatic Literary Work
UNITED STATES COPYRIGHT OFFICE

TXU 1-036-064



TXU 1-036-064

EFFECTIVE DATE OF REGISTRATION

JUN 14 2002

Month Day Year

OFFICIAL SEAL

REGISTER OF COPYRIGHTS
United States of America

DO NOT WRITE ABOVE THIS LINE. IF YOU NEED MORE SPACE, USE A SEPARATE CONTINUATION SHEET.

1

TITLE OF THIS WORK ▼

Cisco IOS 12.0

PREVIOUS OR ALTERNATIVE TITLES ▼ Cisco IOS Release 12.0; Cisco IOS Version 12.0; Cisco Internetwork Operating System 12.0; Cisco Internetwork Operating System Release 12.0; Cisco Internetwork Operating System Version 12.0

PUBLICATION AS A CONTRIBUTION If this work was published as a contribution to a periodical, serial, or collection, give information about the collective work in which the contribution appeared. Title of Collective Work ▼

If published in a periodical or serial give: Volume ▼

Number ▼

Issue Date ▼

On Pages ▼

2NAME OF AUTHOR ▼
a Cisco Systems, Inc.DATES OF BIRTH AND DEATH
Year Born ▼ Year Died ▼

Was this contribution to the work a "work made for hire"?

 Yes NoAUTHOR'S NATIONALITY OR DOMICILE
Name of Country

OR Citizen of ▶

Domiciled in ▶ United States

WAS THIS AUTHOR'S CONTRIBUTION TO THE WORK
If the answer to either of these questions is "Yes," see detailed instructions.
Anonymous? Yes No
Pseudonymous? Yes No**NOTE**

Under the law, the "author" of a "work made for hire" is generally the employer, not the employee (see instructions). For any part of this work that was "made for hire," check "Yes" in the space provided, give the employer (or other person for whom the work was prepared) as "Author" of that part, and leave the space for dates of birth and death blank.

NAME OF AUTHOR ▼
See Attached Form TX/CON for Additional AuthorsDATES OF BIRTH AND DEATH
Year Born ▼ Year Died ▼

Was this contribution to the work a "work made for hire"?

 Yes NoAUTHOR'S NATIONALITY OR DOMICILE
Name of Country

OR Citizen of ▶

Domiciled in ▶

WAS THIS AUTHOR'S CONTRIBUTION TO THE WORK
If the answer to either of these questions is "Yes," see detailed instructions.
Anonymous? Yes No
Pseudonymous? Yes NoNATURE OF AUTHORSHIP Briefly describe nature of material created by this author in which copyright is claimed. ▼
New and revised computer code and accompanying documentation

NAME OF AUTHOR ▼

DATES OF BIRTH AND DEATH
Year Born ▼ Year Died ▼

Was this contribution to the work a "work made for hire"?

 Yes NoAUTHOR'S NATIONALITY OR DOMICILE
Name of Country

OR Citizen of ▶

Domiciled in ▶

WAS THIS AUTHOR'S CONTRIBUTION TO THE WORK
If the answer to either of these questions is "Yes," see detailed instructions.
Anonymous? Yes No
Pseudonymous? Yes No

NATURE OF AUTHORSHIP Briefly describe nature of material created by this author in which copyright is claimed. ▼

NAME OF AUTHOR ▼

DATES OF BIRTH AND DEATH
Year Born ▼ Year Died ▼

Was this contribution to the work a "work made for hire"?

 Yes NoAUTHOR'S NATIONALITY OR DOMICILE
Name of Country

OR Citizen of ▶

Domiciled in ▶

WAS THIS AUTHOR'S CONTRIBUTION TO THE WORK
If the answer to either of these questions is "Yes," see detailed instructions.
Anonymous? Yes No
Pseudonymous? Yes No

NATURE OF AUTHORSHIP Briefly describe nature of material created by this author in which copyright is claimed. ▼

3YEAR IN WHICH CREATION OF THIS WORK WAS COMPLETED
1998

This information must be given in all cases.

b DATE AND NATION OF FIRST PUBLICATION OF THIS PARTICULAR WORK
Complete this information Month ▶ Day ▶ Year ▶ Nation ▶**4**

COPYRIGHT CLAIMANT(S) Name and address must be given even if the claimant is the same as the author given in space 2. ▼

Cisco Technology, Inc.
170 West Tasman Drive
San Jose, CA 95134

See instructions before completing this space.

TRANSFER If the claimant(s) named here in space 4 is (are) different from the author(s) named in space 2, give a brief statement of how the claimant(s) obtained ownership of the copyright. ▼

By agreement

APPLICATION RECEIVED
JUN 14 2002ONE DEPOSIT RECEIVED
JUN 14 2002

TWO DEPOSITS RECEIVED

FUND RECEIVED

DO NOT WRITE HERE
Page 1 of 4 pages

MORE ON BACK ▶ • Complete all applicable spaces (numbers 5-9) on the reverse side of this page.

• See detailed instructions.

• Sign the form at line 8.

EXAMINED BY	TMS	FORM TX
CHECKED BY		
<input type="checkbox"/> CORRESPONDENCE	FOR	
<input checked="" type="checkbox"/> Yes	COPYRIGHT OFFICE USE ONLY	

DO NOT WRITE ABOVE THIS LINE. IF YOU NEED MORE SPACE, USE A SEPARATE CONTINUATION SHEET.

PREVIOUS REGISTRATION Has registration for this work, or for an earlier version of this work, already been made in the Copyright Office?

 Yes No If your answer is "Yes," why is another registration being sought? (Check appropriate box.) ▼

- a. This is the first published edition of a work previously registered in unpublished form.
 b. This is the first application submitted by this author as copyright claimant.
 c. This is a changed version of the work, as shown by space 6 on this application.

If your answer is "Yes," give: Previous Registration Number ▶

Pending

Year of Registration ▶

2002

5

DERIVATIVE WORK OR COMPILE

Preexisting Material Identify any preexisting work or works that this work is based on or incorporates. ▼

Prior works by claimant and preexisting third party computer code

a 6

See instructions
before completing
this space.

Material Added to This Work Give a brief, general statement of the material that has been added to this work and in which copyright is claimed. ▼

New and revised computer code and accompanying documentation

b

DEPOSIT ACCOUNT If the registration fee is to be charged to a Deposit Account established in the Copyright Office, give name and number of Account.
Name ▼ Account Number ▼

a 7

CORRESPONDENCE Give name and address to which correspondence about this application should be sent. Name/Address/Apt/City/State/ZIP ▼

b

Tu T. Tsao, Esq.
 Fenwick & West LLP
 2 Palo Alto Square
 Palo Alto, CA 94306

Area code and daytime telephone number ▶ (650) 858-7696

Fax number ▶

(650) 494-1417

Email ▶ ttsao@fenwick.com

CERTIFICATION I, the undersigned, hereby certify that I am the

Check only one ▶

- { author
 other copyright claimant
 owner of exclusive right(s)
 authorized agent of Cisco Technology, Inc.

Name of author or other copyright claimant, or owner of exclusive right(s) ▲

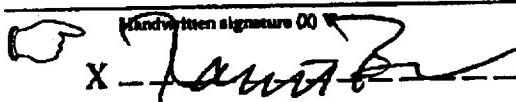
of the work identified in this application and that the statements made by me in this application are correct to the best of my knowledge.

8

Typed or printed name and date ▼ If this application gives a date of publication in space 3, do not sign and submit it before that date.

Robert A. Barr, Worldwide Patent Counsel

Date ▶



Certificate will be mailed in window envelope to this address:

Name ▼ Susanne S. Morales, Paralegal / Fenwick & West LLP
 Number/Street/Apt ▼
 2 Palo Alto Square
 City/State/ZIP ▼
 Palo Alto, CA 94306

YOU MUST
 • Complete all necessary spaces
 • Sign your application in space 8
SEND ALL 3 ELEMENTS IN THE SAME PACKAGE
 1. Application form
 2. Nonrefundable filing fee in check or money order As of
 payable to Register of Copyrights July 1, 1998,
 3. Deposit material the
MAIL TO
 Library of Congress
 Copyright Office
 101 Independence Avenue, S.E.
 Washington, D.C. 20559-6000
 Filing fee for Form TX is \$30.

9

CONTINUATION SHEET FOR APPLICATION FORMS

FORM TX /CON
UNITED STATES COPYRIGHT OFFICE

TXU 1-036-064

ST. 2001636464

P	A	P	U	S	E	G	S	E	S	R	S	R	T	X	U	V	A	V	A
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

EFFECTIVE DATE OF REGISTRATION

JUN 14 2002

(Month) (Day) (Year)

CONTINUATION SHEET RECEIVED

JUN 14 2002

Page 3 of 4 pages

DO NOT WRITE ABOVE THIS LINE. FOR COPYRIGHT OFFICE USE ONLY

IDENTIFICATION OF CONTINUATION SHEET: This sheet is a continuation of the application for copyright registration on the basic form submitted for the following work:

- **TITLE:** (Give the title as given under the heading "Title of this Work" in Space 1 of the basic form.)

Cisco IOS 12.0

- **NAME(S) AND ADDRESS(ES) OF COPYRIGHT CLAIMANT(S):** (Give the name and address of at least one copyright claimant as given in Space 4 of the basic form or Space 2 of any of the Short Forms PA, TX, or VA.)

Cisco Technology, Inc., 170 West Tasman Drive, San Jose, CA 95134

A
Identification
of
Application

NAME OF AUTHOR ▼
(See Space C)

DATES OF BIRTH AND DEATH
Year Born▼ Year Died▼

d

Was this contribution to the work AUTHOR'S NATIONALITY OR DOMICILE a "work made for hire"? Name of Country

Yes
 No

OR Citizen of ► _____
Domiciled in ► _____

WAS THIS AUTHOR'S CONTRIBUTION TO THE WORK
Anonymous? Yes No If the answer to either of these questions is "Yes," see detailed instructions.
Pseudonymous? Yes No

B
Continuation
of Space 2

NATURE OF AUTHORSHIP Briefly describe nature of the material created by the author in which copyright is claimed. ▼

NAME OF AUTHOR ▼

DATES OF BIRTH AND DEATH
Year Born▼ Year Died▼

e

Was this contribution to the work AUTHOR'S NATIONALITY OR DOMICILE a "work made for hire"? Name of Country

Yes
 No

OR Citizen of ► _____
Domiciled in ► _____

WAS THIS AUTHOR'S CONTRIBUTION TO THE WORK
Anonymous? Yes No If the answer to either of these questions is "Yes," see detailed instructions.
Pseudonymous? Yes No

NATURE OF AUTHORSHIP Briefly describe nature of the material created by the author in which copyright is claimed. ▼

NAME OF AUTHOR ▼

DATES OF BIRTH AND DEATH
Year Born▼ Year Died▼

f

Was this contribution to the work AUTHOR'S NATIONALITY OR DOMICILE a "work made for hire"? Name of Country

Yes
 No

OR Citizen of ► _____
Domiciled in ► _____

WAS THIS AUTHOR'S CONTRIBUTION TO THE WORK
Anonymous? Yes No If the answer to either of these questions is "Yes," see detailed instructions.
Pseudonymous? Yes No

NATURE OF AUTHORSHIP Briefly describe nature of the material created by the author in which copyright is claimed. ▼

Use the reverse side of this sheet if you need more space for continuation of Spaces 1, 4, or 5 of the basic form or for the
Chancery DA TY or VA

CONTINUATION OF (Check which): Space 1 Space 4 Space 6 Space 2b

Name of Author	Work for Hire	Domicile	Anonymous	Pseudo-anonymous	Nature of Contribution
Adecco Employment Services	Yes	United States	Yes	No	Computer code
Avnisoft Corporation	Yes	United States	Yes	No	Computer code
HCL Consulting Limited	Yes	United States	Yes	No	Computer code
HCL America, Inc.	Yes	India	Yes	No	Computer code
H.L. Yoh Company LLC	Yes	United States	Yes	No	Computer code
Aquas	Yes	United States	Yes	No	Computer code
Metaplex, Inc.	Yes	United States	Yes	No	Computer code
Rapidigm	Yes	United States	Yes	No	Computer code
Wipro Limited	Yes	India	Yes	No	Computer code
Lasselle-Ramsay	Yes	United States	Yes	No	Documentation
Oakhill Publications/ Computer Education Consulting	Yes	United States	Yes	No	Documentation
Rick Barron	No	United States	Yes	No	Documentation
On-Call Consultants, Inc.	Yes	United States	Yes	No	Documentation
Judy Melanson	No	United States	Yes	No	Documentation

C
Continuation
of other
Spaces

Certificate
will be
mailed in
window
envelope
to this
address:

Name ▼
Susanne S. Morales, Paralegal / Fenwick & West LLP

Number/Stree/Apt ▼

2 Palo Alto Square

City/State/ZIP ▼

Palo Alto, CA 94306

YOU MUST
• Complete all necessary spaces
• Sign your application

**SEND ALL 3 ELEMENTS
IN THE SAME PACKAGE**

1. Application form
2. Nonrefundable fee in check or money order payable to Register of Copyrights
3. Deposit Material

MAIL TO
Library of Congress, Copyright Office
101 Independence Avenue, S.E.
Washington, D.C. 20559-6000

Fees are effective
through June 30,
2002. After that date,
check the Copyright
Office Website at
www.loc.gov/copyrightright
707-354-5000 for current
fee information.

EXHIBIT F

TX TXU PA PAU VA VAU SR SRU RE
EFFECTIVE DATE OF SUPPLEMENTARY REGISTRATION

Month Day Year

DO NOT WRITE ABOVE THIS LINE. IF YOU NEED MORE SPACE, USE A SEPARATE CONTINUATION SHEET.

A Title of Work ▼

Cisco IOS 12.1

Registration Number of the Basic Registration ▼ TXU 1-036-066	Year of Basic Registration ▼ 2002
Name(s) of Author(s) ▼ Please see Space D for list of author names	Name(s) of Copyright Claimant(s) ▼ Cisco Technology, Inc.

B Location and Nature of Incorrect Information in Basic Registration ▼

Line Number	Line Heading or Description	Name of Author
Incorrect Information as It Appears in Basic Registration ▼		

Cisco Systems, Inc.

Corrected Information ▼

Cisco Systems Sales & Services, Inc.

Explanation of Correction ▼

correct name of author

C Location and Nature of Information in Basic Registration to be Amplified ▼

Line Number	Line Heading or Description	Name of Author
Amplified Information and Explanation of Information ▼		

Please add the following to the list of authors:

Name of Author: Cisco Technology, Inc.

Work for Hire: Yes

Domicile: United States

Anonymous: No

Pseudonymous: No

Nature of Contribution: Computer code and documentation

MORE ON BACK ▶

- Complete all applicable spaces (D-G) on the reverse side of this page.
- See detailed instructions.
- Sign the form at Space F.

DO NOT WRITE HERE

Page 1 of _____ pages

FUND RECEIVED DATE

EXAMINED BY

CORRESPONDENCE

REFERENCE TO THIS REGISTRATION ADDED TO
BASIC REGISTRATION YES NO

FOR
COPYRIGHT
OFFICE
USE
ONLY**DO NOT WRITE ABOVE THIS LINE. IF YOU NEED MORE SPACE, USE A SEPARATE CONTINUATION SHEET.**Continuation of: Part B or Part C Part A

Cisco Systems, Inc.
 ABE Staffing Services, Inc.
 Adecco Employment Services
 A.S.K. Office Personnel Solutions
 Computer People
 Cotelligent
 Devsoft Corporation
 HCL America, Inc.
 HCL Consulting Limited
 IT & E Corporation
 Ma Foi Management Consultants Limited
 Maprik Holdings Pty Ltd
 Metaplex, Inc.

Pipelink
 Rapidigm
 Softsol Resources, Inc.
 Wipro Limited
 Lasselle-Ramsay
 Oakhill Publications / Computer Education
 Consulting
 Essential Solutions
 Rick Barron

Correspondence: Give name and address to which correspondence about this application should be sent.

Tu T. Tsao, Esq.
 Fenwick & West LLP
 601 California Street
 Mountain View, CA 94041

Phone (650) 335-7696

Fax (650) 938-5200

Email tttsao@fenwick.com**Deposit Account:** If the registration fee is to be charged to a Deposit Account established in the Copyright Office, give name and number of Account.

Name _____

Account Number _____

Certification* I, the undersigned, hereby certify that I am the: (Check only one)

author owner of exclusive right(s)
 other copyright claimant duly authorized agent of Cisco Technology, Inc.

Name of author or other copyright claimant, or owner of exclusive right(s) ▲

of the work identified in this application and that the statements made by me in this application are correct to the best of my knowledge.

Typed or printed name ▼ Robert A. Barr, Worldwide Patent Counsel

Date ▼

1-8-03

Handwritten signature (X) ▼

Certificate
will be
mailed in
window
envelope
to this
address:Name ▼
Susanne S. Morales, Paralegal / Fenwick & West LLP

Number/Street/Apt ▼

801 California Street

City/State/ZIP ▼

Mountain View, CA 94041

INSTRUCTIONS

- Complete all necessary spaces
 - Sign your application in Space F
- SEND YOUR FILLED
FEE PAYMENT PACKAGE

1. Application form
2. Nonrefundable filing fee in check or money order payable to Register of Copyrights

TELE: 202

Library of Congress
 Copyright Office
 101 Independence Avenue, S.E.,
 Washington, D.C. 20508-6000

Fees are subject to
 change. For current
 fees, contact the
 Copyright Office
 website at
www.copyright.gov
 or call the Copyright
 Office, at (202) 707-3000.

*17 U.S.C. § 506(e): Any person who knowingly makes a false representation of a material fact in the application for copyright registration provided for by section 409, or in any written statement filed in connection with the application, shall be fined not more than \$2,500.

EXAMINED BY	TMS	FORM TX
CHECKED BY		
<input type="checkbox"/> CORRESPONDENCE		FOR COPYRIGHT OFFICE USE ONLY
<input type="checkbox"/> Yes		

DO NOT WRITE ABOVE THIS LINE. IF YOU NEED MORE SPACE, USE A SEPARATE CONTINUATION SHEET.

PREVIOUS REGISTRATION Has registration for this work, or for an earlier version of this work, already been made in the Copyright Office?

- Yes No If your answer is "Yes," why is another registration being sought? (Check appropriate box.) ▼
- a. This is the first published edition of a work previously registered in unpublished form.
 - b. This is the first application submitted by this author as copyright claimant.
 - c. This is a changed version of the work, as shown by space 6 on this application.

If your answer is "Yes," give Previous Registration Number ►

Pending

Year of Registration ►

2002

5

DERIVATIVE WORK OR COMPILATION

Preexisting Material Identify any preexisting work or works that this work is based on or incorporates. ▼

Prior works by claimant and preexisting third party computer code

a 6

See instructions
before completing
this space.Material Added to This Work Give a brief, general statement of the material that has been added to this work and in which copyright is claimed. ▼
New and revised computer code and accompanying documentation

b

DEPOSIT ACCOUNT If the registration fee is to be charged to a Deposit Account established in the Copyright Office, give name and number of Account.
Name ▼ Account Number ▼

a 7

CORRESPONDENCE Give name and address to which correspondence about this application should be sent. Name/Address/Apt/City/State/ZIP ▼

Tu T. Tsao, Esq.
Fenwick & West LLP
2 Palo Alto Square
Palo Alto, CA 94306

Area code and daytime telephone number ► (650) 858-7696

Fax number ► (650) 494-1417

Email ► tttsao@fenwick.com

b

7

8

CERTIFICATION I, the undersigned, hereby certify that I am the

Check only one ►

- author
- other copyright claimant
- owner of exclusive right(s)
- authorized agent of Cisco Technology, Inc.

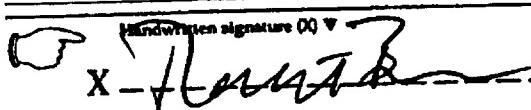
Name of author or other copyright claimant, or owner of exclusive right(s) ▲

of the work identified in this application and that the statements made
by me in this application are correct to the best of my knowledge.

Typed or printed name and date ▼ If this application gives a date of publication in space 3, do not sign and submit it before that date.

Robert A. Barr, Worldwide Patent Counsel

Date ►



Handwritten signature DD ▼
X - Robert A. Barr

Certificate
will be
mailed in
window
envelope
to this
address:

Name ▼ Susanne S. Morales, Paralegal / Fenwick & West LLP
Number/Street/Apt ▼
2 Palo Alto Square
City/State/ZIP ▼
Palo Alto, CA 94306

YOU MUST

- Complete all necessary spaces
- Sign your application in space 8

**SEND ALL ELEMENTS
IN THE SAME PACKAGE**

1. Application form
2. Nonrefundable filing fee in check or money order As of
payable to Register of Copyrights July 1,
1999,
3. Deposit material the
MAIL TO:
Library of Congress
Copyright Office
101 Independence Avenue, S.E.
Washington, D.C. 20559-6000
Billing
fee for
Form TX
is \$30.

*17 U.S.C. § 506(e): Any person who knowingly makes a false representation of a material fact in the application for copyright registration provided for by section 408, or in any written statement filed in connection with the application, shall be fined not more than \$2,500.
June 1999—200,000
WEB REV: June 1999

U.S. GOVERNMENT PRINTING OFFICE: 1999-454-87949

9

CONTINUATION SHEET FOR APPLICATION FORMS

- This Continuation Sheet is used in conjunction with Forms CA, PA, SE, SR, TX, and VA, only. Indicate which basic form you are continuing in the space in the upper right-hand corner.
- If at all possible, try to fit the information called for into the spaces provided on the basic form.
- If you do not have enough space for all the information you need to give on the basic form, use this Continuation Sheet and submit it with the basic form.
- If you submit this Continuation Sheet, clip (do not tape or staple) it to the basic form and fold the two together before submitting them.
- Space A of this sheet is intended to identify the basic application. Space B is a continuation of Space 2 on the basic application. Space C is not applicable to Short forms. Space C (on the reverse side of this sheet) is for the continuation of Spaces 1, 4, or 6 on the basic application or for the continuation of Space 1 on any of the three Short Forms PA, TX, or VA.

DO NOT WRITE ABOVE THIS LINE. FOR COPYRIGHT OFFICE USE ONLY

eFORM TX /CON
UNITED STATES COPYRIGHT OFFICE

TXU 1-036-066



PAPAUSESEGSELSRISRU TX TXUVA VAU

EFFECTIVE DATE OF REGISTRATION

JUN 1 4 2002

(Month) (Day) (Year)

CONTINUATION SHEET RECEIVED

JUN 1 4 2002

Page 3 of 4 pages

A
Identification
of
Application

IDENTIFICATION OF CONTINUATION SHEET: This sheet is a continuation of the application for copyright registration on the basic form submitted for the following work:

- TITLE: (Give the title as given under the heading "Title of this Work" in Space 1 of the basic form.)

Cisco IOS 12.1

- NAME(S) AND ADDRESS(ES) OF COPYRIGHT CLAIMANT(S): (Give the name and address of at least one copyright claimant as given in Space 4 of the basic form or Space 2 of any of the Short Forms PA, TX, or VA.)
Cisco Technology, Inc., 170 West Tasman Drive, San Jose, CA 95134

B
Continuation
of Space 2

NAME OF AUTHOR ▼
(See Space C)

DATES OF BIRTH AND DEATH
Year Born▼ Year Died▼

B Was this contribution to the work **AUTHOR'S NATIONALITY OR DOMICILE**
a "work made for hire"? Name of Country

- Yes
 No

OR Citizen of ► _____
Domiciled in ► _____

**WAS THIS AUTHOR'S CONTRIBUTION TO
THE WORK**
Anonymous? Yes No If the answer to either
of these questions is
"Yes," see detailed
instructions.
Pseudonymous? Yes No

NATURE OF AUTHORSHIP Briefly describe nature of the material created by the author in which copyright is claimed. ▼

NAME OF AUTHOR ▼

DATES OF BIRTH AND DEATH
Year Born▼ Year Died▼

e Was this contribution to the work **AUTHOR'S NATIONALITY OR DOMICILE**
a "work made for hire"? Name of Country

- Yes
 No

OR Citizen of ► _____
Domiciled in ► _____

**WAS THIS AUTHOR'S CONTRIBUTION TO
THE WORK**
Anonymous? Yes No If the answer to either
of these questions is
"Yes," see detailed
instructions.
Pseudonymous? Yes No

NATURE OF AUTHORSHIP Briefly describe nature of the material created by the author in which copyright is claimed. ▼

NAME OF AUTHOR ▼

DATES OF BIRTH AND DEATH
Year Born▼ Year Died▼

f Was this contribution to the work **AUTHOR'S NATIONALITY OR DOMICILE**
a "work made for hire"? Name of Country

- Yes
 No

OR Citizen of ► _____
Domiciled in ► _____

**WAS THIS AUTHOR'S CONTRIBUTION TO
THE WORK**
Anonymous? Yes No If the answer to either
of these questions is
"Yes," see detailed
instructions.
Pseudonymous? Yes No

NATURE OF AUTHORSHIP Briefly describe nature of the material created by the author in which copyright is claimed. ▼

Use the reverse side of this sheet if you need more space for continuation of Spaces 1, 4, or 6 of the basic form or for the
continuation of Space 1 on any of the Short Forms PA, TX, or VA.

CONTINUATION OF (Check which):		<input type="checkbox"/> Space 1	<input type="checkbox"/> Space 4	<input type="checkbox"/> Space 6	<input checked="" type="checkbox"/> Space 2b	
Name of Author	Work for Hire	Domicile	Anonymous	Pseudo-nymous	Nature of Contribution	Continuation of other Spaces
ABE Staffing Services, Inc.	Yes	United States	Yes	No	Computer code	C
Adecco Employment Services	Yes	United States	Yes	No	Computer code	
A.S.K. Office Personnel Solutions	Yes	Australia	Yes	No	Computer code	
Computer People	Yes	United States	Yes	No	Computer code	
Cotelligent	Yes	United States	Yes	No	Computer code	
Devsoft Corporation	Yes	United States	Yes	No	Computer code	
HCL America, Inc.	Yes	United States	Yes	No	Computer code	
HCL Consulting Limited	Yes	India	Yes	No	Computer code	
IT & E Corporation	Yes	United States	Yes	No	Computer code	
Ma Foi Management Consultants Limited	Yes	India	Yes	No	Computer code	
Maprik Holdings Pty Ltd	Yes	Australia	Yes	No	Computer code	
Metaplex, Inc.	Yes	United States	Yes	No	Computer code	
Pipelink	Yes	United States	Yes	No	Computer code	
Rapidigm		India				
Softsol Resources, Inc.	Yes	United States	Yes	No	Computer code	
Wipro Limited	Yes	United States	Yes	No	Documentation	
Lasselle-Ramsay	Yes	United States	Yes	No	Documentation	
Oakhill Publications/ Computer Education Consulting	Yes	United States	Yes	No	Documentation	
Essential Solutions	Yes	United States	Yes	No	Documentation	
Rick Barron	No	United States	Yes	No	Documentation	

Certificate will be mailed in window envelope to this address:

Name ▼ Susanne S. Morales, Paralegal / Fenwick & West LLP

Number/Street/Apt ▼

2 Palo Alto Square

City/State/ZIP ▼

Palo Alto, CA 94306

YOU MUST
• Complete all necessary spaces
• Sign your application

SEND ALL 3 ELEMENTS
IN THE SAME PACKAGE

1. Application form
2. Nonrefundable fee in check or money order payable to Register of Copyrights
3. Deposit Material

MAIL TO
Library of Congress, Copyright Office
101 Independence Avenue, S.E.
Washington, D.C. 20559-6000

Fees are effective through June 30, 2002. After that date, check the Copyright office Website at [www.usccopyright.gov](http://www.uscopyright.gov) or call (202) 707-3009 for current fee information.

EXHIBIT G

Copyright Office fees are subject to change.
For current fees, check the Copyright Office website at www.copyright.gov, write the Copyright Office, or call (202) 707-3000.

FORM CA

For Supplementary Registration
UNITED STATES COPYRIGHT OFFICE
REGISTRATION NUMBER

TX	TXU	PA	PAU	VA	VAU	SR	SRU	RE
EFFECTIVE DATE OF SUPPLEMENTARY REGISTRATION								

Month Day Year

DO NOT WRITE ABOVE THIS LINE. IF YOU NEED MORE SPACE, USE A SEPARATE CONTINUATION SHEET.

A Title of Work ▼

Cisco IOS 12.2

Registration Number of the Basic Registration ▼ TXu 1-036-065	Year of Basic Registration ▼ 2002
Name(s) of Author(s) ▼ Please see Space D for list of name of authors	Name(s) of Copyright Claimant(s) ▼ Cisco Technology, Inc.

B Location and Nature of Incorrect Information in Basic Registration ▼

Line Number 2a	Line Heading or Description	Name of Author
Incorrect Information as It Appears in Basic Registration ▼		
Cisco Systems, Inc.		
Corrected Information ▼		
Cisco Systems Sales & Services, Inc.		
Explanation of Correction ▼		
correct name of author		

C Location and Nature of Information in Basic Registration to be Amplified ▼

Line Number 2b and C	Line Heading or Description	Name of Author
Amplified Information and Explanation of Information ▼		
Please add the following to the list of author names:		
Name of Author: Cisco Technology, Inc.		
Work for Hire: Yes		
Domicile: United States		
Anonymous: No		
Pseudonymous: No		
Nature of Contribution: Computer code and documentation		

MORE ON BACK ►

- Complete all applicable spaces (D-G) on the reverse side of this page.
- See detailed instructions.
- Sign the form at Space F.

DO NOT WRITE HERE

Page 1 of _____ pages

FUND RECEIVED DATE

EXAMINED BY

CORRESPONDENCE

REFERENCE TO THIS REGISTRATION ADDED TO
BASIC REGISTRATION YES NO

FOR
COPYRIGHT
OFFICE
USE
ONLY

DO NOT WRITE ABOVE THIS LINE. IF YOU NEED MORE SPACE, USE A SEPARATE CONTINUATION SHEET.

Continuation of: Part B or Part C Part A

Cisco Systems, Inc.
 ABE Staffing Services, Inc.
 Adecco Employment Services
 Acionyx, Incorporated
 Greenwood Group, dba Manpower
 Technical Services
 HCL America, Inc.
 HCL Consulting Limited
 H.L. Yoh Company LLC
 Hughes Software Systems USA
 InfoSys Technologies Limited
 Insight Solutions, Inc.
 IT & E Corporation

Ma Foi Management Consultants Limited
 Metalogic, S.A.R.L.
 Metaplex, Inc.
 Rapidigm
 Savvy System Consultants
 Ultimate Technology, Inc.
 Wipro Limited
 Lasselle-Ramsay
 Oakhill Publications / Computer Education Consulting
 Rick Barron

D

E

F

Correspondence: Give name and address to which correspondence about this application should be sent.

Tu T. Tsao, Esq.
 Fenwick & West LLP
 801 California Street
 Mountain View, CA 94041

Phone (650) 335-7696

Fax (650) 938-5200

Email tttsao@fenwick.com

Deposit Account: If the registration fee is to be charged to a Deposit Account established in the Copyright Office, give name and number of Account:

Name _____

Account Number _____

Certification* I, the undersigned, hereby certify that I am the: (Check only one)

author owner of exclusive right(s)
 other copyright claimant duly authorized agent of Cisco Technology, Inc.

Name of author or other copyright claimant, or owner of exclusive right(s) ▲

of the work identified in this application and that the statements made by me in this application are correct to the best of my knowledge.

Typed or printed name ▼ Robert A. Barr, Worldwide Patent Counsel

Date ▼ 1-8-03

Handwritten signature (X) ▼ Certificate
will be
mailed in
window
envelope
to this
address:

Name ▼	Susanne S. Morales, Paralegal / Fenwick & West LLP
Number/Street/Apt ▼	801 California Street
City/State/ZIP ▼	Mountain View, CA 94041

YOU MUST	• Complete all necessary spaces. • Sign your application in Space F.
SIGN YOUR APPLICATION IN THE SPACE PROVIDED	
1. Application form 2. Nonrefundable filing fee in check or money order payable to Register of Copyrights U.S. GOVERNMENT PRINTING OFFICE Library of Congress Copyright Office 101 Independence Avenue, S.E. Washington, D.C. 20590-6000	

Please see legend in
changes. For current
form, check the
Copyright Office
Web site at
www.copyright.gov,
write the Copyright
Office, or call
(202) 707-9000.

*17 U.S.C. § 506(e): Any person who knowingly makes a false representation of a material fact in the application for copyright registration provided for by section 408, or in any written statement filed in connection with the application, shall be fined not more than \$2,500.

CERTIFICATE OF REGISTRATION

OFFICIAL SEAL

This Certificate issued under the seal of the Copyright Office in accordance with title 17, United States Code, attests that registration has been made for the work identified below. The information on this certificate has been made a part of the Copyright Office records.

FORM TX
For a Nondramatic Literary Work
UNITED STATES COPYRIGHT OFFICE



RE

TXU 1-036-D65

PTAB01036D65

EFFECTIVE DATE OF REGISTRATION

JUN 14 2002

Month Day Year

REGISTER OF COPYRIGHTS
United States of America

DO NOT WRITE ABOVE THIS LINE. IF YOU NEED MORE SPACE, USE A SEPARATE CONTINUATION SHEET.

1

TITLE OF THIS WORK ▼

Cisco IOS 12.2

PREVIOUS OR ALTERNATIVE TITLES ▼ Cisco IOS Release 12.2; Cisco IOS Version 12.2; Cisco Internetwork Operating System 12.2; Cisco Internetwork Operating System Release 12.2; Cisco Internetwork Operating System Version 12.2

PUBLICATION AS A CONTRIBUTION If this work was published as a contribution to a periodical, serial, or collection, give information about the collective work in which the contribution appeared. Title of Collective Work ▼

If published in a periodical or serial give: Volume ▼	Number ▼	Issue Date ▼	On Page ▼
---	----------	--------------	-----------

2

NAME OF AUTHOR ▼
a Cisco Systems, Inc.

DATES OF BIRTH AND DEATH
Year Born ▼ Year Died ▼Was this contribution to the work a "work made for hire"? Yes No

AUTHOR'S NATIONALITY OR DOMICILE
Name of Country
OR Citizen of ▶ Domiciled in ▶ United States

WAS THIS AUTHOR'S CONTRIBUTION TO THE WORK
Anonymous? Yes No
Pseudonymous? Yes No
If the answer to either of these questions is "Yes," see detailed instructions.

NOTE

Under the law, the "author" of a "work made for hire" is generally the employer, not the employee (see instructions). For any part of this work that was "made for hire," check "Yes" in the space provided, give the employer (or other person for whom the work was prepared) as "Author" of that part, and leave the space for dates of birth and death blank.

NATURE OF AUTHORSHIP Briefly describe nature of material created by this author in which copyright is claimed. ▼
New and revised computer code and accompanying documentationDATES OF BIRTH AND DEATH
Year Born ▼ Year Died ▼NAME OF AUTHOR ▼
b See Attached Form TX/CON for Additional AuthorsWAS THIS AUTHOR'S CONTRIBUTION TO THE WORK
Anonymous? Yes No
Pseudonymous? Yes No
If the answer to either of these questions is "Yes," see detailed instructions.Was this contribution to the work a "work made for hire"? Yes No

AUTHOR'S NATIONALITY OR DOMICILE
Name of Country
OR Citizen of ▶ Domiciled in ▶

NATURE OF AUTHORSHIP Briefly describe nature of material created by this author in which copyright is claimed. ▼

DATES OF BIRTH AND DEATH
Year Born ▼ Year Died ▼NAME OF AUTHOR ▼
c

WAS THIS AUTHOR'S CONTRIBUTION TO THE WORK
Anonymous? Yes No
Pseudonymous? Yes No
If the answer to either of these questions is "Yes," see detailed instructions.

Was this contribution to the work a "work made for hire"? Yes No

AUTHOR'S NATIONALITY OR DOMICILE
Name of Country
OR Citizen of ▶ Domiciled in ▶

NATURE OF AUTHORSHIP Briefly describe nature of material created by this author in which copyright is claimed. ▼

3

YEAR IN WHICH CREATION OF THIS WORK WAS COMPLETED
a 2001 1 Year in all cases.

DATE AND NATION OF FIRST PUBLICATION OF THIS PARTICULAR WORK

b Complete this information Month ▶ Day ▶ Year ▶ Nation ▶

4
See instructions before completing this space.

COPYRIGHT CLAIMANT(S) Name and address must be given even if the claimant is the same as the author given in space 2. ▼

Cisco Technology, Inc.
170 West Tasman Drive
San Jose, CA 95134

APPLICATION RECEIVED
JUN 14 2002

ONE DEPOSIT RECEIVED

JUN 14, 2002

TWO DEPOSITS RECEIVED

FUND RECEIVED

DO NOT WRITE HERE

TRANSFER If the claimant(s) named here in space 4 is (are) different from the author(s) named in space 2, give a brief statement of how the claimant(s) obtained ownership of the copyright. ▼

By agreement

MORE ON BACK ▶ • Complete all applicable spaces (numbers 5-8) on the reverse side of this page.
• See detailed instructions.

• Sign the form at line 9.

DO NOT WRITE HERE
Page 1 of 7 Pages

EXAMINED BY	TMS	FORM TX
CHECKED BY		
<input type="checkbox"/> CORRESPONDENCE	FOR COPYRIGHT OFFICE USE ONLY	
<input checked="" type="checkbox"/> Yes		

DO NOT WRITE ABOVE THIS LINE. IF YOU NEED MORE SPACE, USE A SEPARATE CONTINUATION SHEET.

PREVIOUS REGISTRATION Has registration for this work, or for an earlier version of this work, already been made in the Copyright Office?

 Yes No If your answer is "Yes," why is another registration being sought? (Check appropriate box.) ▼

- a. This is the first published edition of a work previously registered in unpublished form.
 b. This is the first application submitted by this author as copyright claimant.
 c. This is a changed version of the work, as shown by space 6 on this application.

If your answer is "Yes," give Previous Registration Number ►

Pending

Year of Registration ►

2002

5

DERIVATIVE WORK OR COMPILATION

Preexisting Material Identify any preexisting work or works that this work is based on or incorporates. ▼

Prior works by claimant and preexisting third party computer code

a 6

See instructions
before completing
this space.Material Added to This Work Give a brief, general statement of the material that has been added to this work and in which copyright is claimed. ▼
New and revised computer code and accompanying documentation

b

DEPOSIT ACCOUNT If the registration fee is to be charged to a Deposit Account established in the Copyright Office, give name and number of Account.
Name ▼ Account Number ▼

a

7

CORRESPONDENCE Give name and address to which correspondence about this application should be sent. Name/Address/Apt/City/State/ZIP ▼

b

b

Tu T. Tsao, Esq.
Fenwick & West LLP
2 Palo Alto Square
Palo Alto, CA 94306

Area code and daytime telephone number ► (650) 858-7696

Fax number ► (650) 494-1417

Email ► tttsao@fenwick.com

CERTIFICATION I, the undersigned, hereby certify that I am the

Check only one ►

- author
 other copyright claimant
 owner of exclusive right(s)
 authorized agent of Cisco Technology, Inc.

Name of author or other copyright claimant, or owner of exclusive right(s) ▲

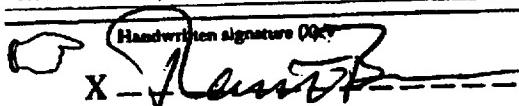
8

of the work identified in this application and that the statements made
by me in this application are correct to the best of my knowledge.

Typed or printed name and date ▼ If this application gives a date of publication in space 3, do not sign and submit it before that date.

Robert A. Barr, Worldwide Patent Counsel

Date ►


 Handwritten signature of Robert A. Barr
Certificate
will be
mailed in
window
envelope
to this
address:
 Name ▼ Susanne S. Morales, Paralegal / Fenwick & West LLP
 Number/Street/Apt ▼ 2 Palo Alto Square
 City/State/ZIP ▼ Palo Alto, CA 94306

YOU MUST	
• Complete all necessary spaces • Sign your application in space 8	
SEND ALL ELEMENTS IN THE SAME PACKAGE	
1. Application form 2. Nonrefundable filing fee in check or money order payable to Register of Copyrights 3. Deposit material	
MAIL TO	As of July 1, 1999, the filing fee for Form TX is \$30.
Library of Congress Copyright Office 101 Independence Avenue, S.E. Washington, D.C. 20559-6000	

9

*17 U.S.C. § 506(a): Any person who knowingly makes a false representation of a material fact in the application for copyright registration provided for by section 408, or in any written statement filed in connection with the application, shall be fined not more than \$2,500.
 June 1999—200,000
 WEB REV: June 1999

U.S. GOVERNMENT PRINTING OFFICE: 1609-454-87848

CONTINUATION SHEET FOR APPLICATION FORMS

- This Continuation Sheet is used in conjunction with Forms CA, PA, SE, SR, TX, and VA, only. Indicate which basic form you are continuing in the space in the upper right-hand corner.
- If at all possible, try to fit the information called for into the spaces provided on the basic form.
- If you do not have enough space for all the information you need to give on the basic form, use this Continuation Sheet and submit it with the basic form.
- If you submit this Continuation Sheet, clip (do not tape or staple) it to the basic form and fold the two together before submitting them.
- Space A of this sheet is intended to identify the basic application. Space B is a continuation of Space 2 on the basic application. Space B is not applicable to Short forms.
- Space C (on the reverse side of this sheet) is for the continuation of Spaces 1, 4, or 6 on the basic application or for the continuation of Space 1 on any of the three Short Forms PA, TX, or VA.

DO NOT WRITE ABOVE THIS LINE. FOR COPYRIGHT OFFICE USE ONLY

FORM TX /CON
UNITED STATES COPYRIGHT OFFICE

TXU 1-036-065

171001560254

PAPA	PAUSE	SEG	SEU	SR	SRM	T	TXU	V	VAU
------	-------	-----	-----	----	-----	---	-----	---	-----

EFFECTIVE DATE OF REGISTRATION

JUN 14 2002

(Month) (Day) (Year)

CONTINUATION SHEET RECEIVED

JUN 14 2002

Page 3 of 4 pages

A
Identification
of
Application

IDENTIFICATION OF CONTINUATION SHEET: This sheet is a continuation of the application for copyright registration on the basic form submitted for the following work:

- TITLE:** (Give the title as given under the heading "Title of this Work" in Space 1 of the basic form.)

Cisco IOS 12.2

- NAME(S) AND ADDRESS(ES) OF COPYRIGHT CLAIMANT(S):** (Give the name and address of at least one copyright claimant as given in Space 4 of the basic form or Space 2 of any of the Short Forms PA, TX, or VA.)
Cisco Technology, Inc., 170 West Tasman Drive, San Jose, CA 95134

B
Continuation
of Space 2

d

Was this contribution to the work AUTHOR'S NATIONALITY OR DOMICILE
a "work made for hire"? Name of Country

- Yes
 No

OR Citizen of ► _____
Domiciled in ► _____

DATES OF BIRTH AND DEATH
Year Born▼ Year Died▼

WAS THIS AUTHOR'S CONTRIBUTION TO
THE WORK
Anonymous? Yes No If the answer to either
of these questions is
"Yes," see detailed
instructions.

Pseudonymous? Yes No If the answer to either
of these questions is
"Yes," see detailed
instructions.

NATURE OF AUTHORSHIP: Briefly describe nature of the material created by the author in which copyright is claimed. ▼

c
NAME OF AUTHOR ▼

DATES OF BIRTH AND DEATH
Year Born▼ Year Died▼

e

Was this contribution to the work AUTHOR'S NATIONALITY OR DOMICILE
a "work made for hire"? Name of Country

- Yes
 No

OR Citizen of ► _____
Domiciled in ► _____

WAS THIS AUTHOR'S CONTRIBUTION TO
THE WORK
Anonymous? Yes No If the answer to either
of these questions is
"Yes," see detailed
instructions.

Pseudonymous? Yes No If the answer to either
of these questions is
"Yes," see detailed
instructions.

NATURE OF AUTHORSHIP: Briefly describe nature of the material created by the author in which copyright is claimed. ▼

f
NAME OF AUTHOR ▼

DATES OF BIRTH AND DEATH
Year Born▼ Year Died▼

f

Was this contribution to the work AUTHOR'S NATIONALITY OR DOMICILE
a "work made for hire"? Name of Country

- Yes
 No

OR Citizen of ► _____
Domiciled in ► _____

WAS THIS AUTHOR'S CONTRIBUTION TO
THE WORK
Anonymous? Yes No If the answer to either
of these questions is
"Yes," see detailed
instructions.

Pseudonymous? Yes No If the answer to either
of these questions is
"Yes," see detailed
instructions.

NATURE OF AUTHORSHIP: Briefly describe nature of the material created by the author in which copyright is claimed. ▼

Use the reverse side of this sheet if you need more space for continuation of Spaces 1, 4, or 6 of the basic form or for the continuation of Space 1 on any of the Short Forms PA, TX, or VA.

C

CONTINUATION OF (Check which):		<input type="checkbox"/> Space 1	<input type="checkbox"/> Space 4	<input type="checkbox"/> Space 6	<input checked="" type="checkbox"/> Space 2b	Nature of Contribution	Continuation of other Spaces
Name of Author	Work for Hire	Domicile	Anonymous	Pseudo- nymous			
ABE Staffing Services, Inc.	Yes	United States	Yes	No	Computer code and documentation		
Adecco Employment Services	Yes	United States	Yes	No	Computer code and documentation		
Acionyx, Incorporated	Yes	United States	Yes	No	Computer code		
Greenwood Group, dba Manpower Technical Services	Yes	United States	Yes	No	Computer code and documentation		
HCL America, Inc.	Yes	United States	Yes	No	Computer code		
HCL Consulting Limited	Yes	United States	Yes	No	Computer code		
H.L. Yoh Company LLC	Yes	United States	Yes	No	Computer code		
Hughes Software Systems USA	Yes	United States	Yes	No	Computer code		
InfoSys Technologies Limited	Yes	United States	Yes	No	Computer code		
Insight Solutions, Inc.	Yes	United States	Yes	No	Computer code		
JT & E Corporation	Yes	United States	Yes	No	Computer code		
Ma Foi Management Consultants Limited	Yes	United States	Yes	No	Computer code		
Metalogic, S.A.R.L.	Yes	United States	Yes	No	Computer code		
Metaplex, Inc.	Yes	United States	Yes	No	Computer code		
Rapidign:	Yes	United States	Yes	No	Computer code		
Savvy System Consultants	Yes	United States	Yes	No	Computer code		
Ultimate Technology, Inc.	Yes	United States	Yes	No	Computer code		
Wipro Limited	Yes	United States	Yes	No	Computer code		
Lasselle-Ramsey	Yes	United States	Yes	No	Documentation		
Oakhill Publications/ Computer Education Consulting	Yes	United States	Yes	No	Documentation		
Rick Barron	No	United States	Yes	No	Documentation		

D

Certificate will be mailed in window envelope to this address:	Name: Susanne S. Morales, Paralegal / Fenwick & West LLP Number/Street/Av: 2 Palo Alto Square City/State/ZIP: Palo Alto, CA 94306	YOU MUST - Complete all necessary spaces - Sign your application SEND ALL ELEMENTS IN THE SAME PACKAGE 1. Application form 2. Nonrefundable fee in check or money order payable to Register of Copyrights 3. Deposit Material MAIL TO Library of Congress, Copyright Office 101 Independence Avenue, S.E. Washington, D.C. 20556-6000	<small>Forms are effective through June 26, 2002. After that date, check the Copyright office Website at www.loc.gov/copyright/. Right on sale (2002) 707-544-5000 for further information.</small>
--	---	--	---

Cisco/Huawei

Exhibit H:
Manual Comparison

Huawei “ip address” Command (1 of 2)

Cisco “ip address” Command (1 of 2)

User Manual – Command Reference (Volume 1) Versatile Routing Platform	IP Address Configuration Commands
* * * *	

1.1.1 ip address

To set a primary or secondary IP address for an interface, use the **ip address** command. To remove an IP address or disable IP processing, use the **no** form of this command.

ip address ip-address mask [secondary]

no ip address [ip-address]

Syntax Description

ip-address IP address.

net-mask Mask for the associated IP subnet. It is all in decimal format divided by dots.

If there is no **ip-address** in the command **no ip address**, delete all the IP address of the interface.

secondary specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address.

Default

No IP address is defined for the interface

User Manual – Command Reference (Volume 1) Versatile Routing Platform	IP Address Configuration Commands
* * * *	

ip address

To set a primary or secondary IP address for an interface, use the **ip address** command. To remove an IP address or disable IP processing, use the **no** form of this command.

ip address ip-address mask [secondary]

no ip address ip-address mask [secondary]

Syntax Description

ip-address IP address.

mask Mask for the associated IP subnet.

secondary (Optional) Specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address.

Default

No IP address is defined for the interface.

Huawei Command Reference, Version 1.5, Volume 1, Module 04, pp. 1-1 to 1-2

<http://datacomm.huawei.com/english/index.html>

[Select “Document Center” link; then select “VRP Command and Configuration Manual” link; then select “Command Reference V1.5”; then select “Command Reference(V1.5)-Volume 1” link.]

Cisco Network Protocols Command Reference, Part 1, Version 11.2, IP Commands, pp. V-57 to V-58

http://www.cisco.com/en/US/products/sw/iosswrel/ps1824/products_command_reference_chapter09186a0080080d98.html
[Select “ip address” link or select PDF file for entire document and go to cited pages]

Huawei “ip address” Command (2 of 2)

Cisco “ip address” Command (2 of 2)

User Manual – Command Reference (Volume 1)	IP Address Configuration Commands
* * *	* * *

Command Mode

Interface configuration mode

Usage Guideline

An interface can have one primary IP address and multiple secondary IP addresses. Packets generated by the software always use the primary IP address. Therefore, all routers and access servers on a segment should share the same primary network number.

Hosts can determine subnet masks using the Internet Control Message Protocol (ICMP) Mask Request message. Routers respond to this request with an ICMP Mask Reply message.

You can disable IP processing on a particular interface by removing its IP address with the no ip address command. If the software detects another host using one of its IP addresses, it will print an error message on the console.

The optional keyword **secondary** allows you to specify an unlimited number of secondary addresses. Secondary addresses are treated like primary addresses, except the system never generates datagrams other than routing updates with secondary source addresses. IP broadcasts and ARP requests are handled properly, as are interface routes in the IP routing table.

Secondary IP addresses can be used in a variety of situations. The following are the most common applications:

- There may not be enough host addresses for a particular network segment. For example, your subnetting allows up to 254 hosts per logical subnet, but on one physical subnet you need to have 300 host addresses. Using secondary IP addresses on the routers or access servers allows you to have two logical subnets using one physical subnet.
- Many older networks were built using Level 2 bridges. The judicious use of secondary addresses can aid in the transition to a subnetted, router-based network. Routers on an older, bridged segment can be easily made aware that there are many subnets on that segment.

Chapter	
User Manual – Command Reference (Volume 1)	IP Address Configuration Commands

* * *	* * *
-------	-------

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

An interface can have one primary IP address and multiple secondary IP addresses. Packets generated by the Cisco IOS software always use the primary IP address. Therefore, all routers and access servers on a segment should share the same primary network number.

Hosts can determine subnet masks using the Internet Control Message Protocol (ICMP) Mask Request message. Routers respond to this request with an ICMP Mask Reply message.

You can disable IP processing on a particular interface by removing its IP address with the no ip address command. If the software detects another host using one of its IP addresses, it will print an error message on the console.

The optional keyword **secondary** allows you to specify an unlimited number of secondary addresses. Secondary addresses are treated like primary addresses, except the system never generates datagrams other than routing updates with secondary source addresses. IP broadcasts and ARP requests are handled properly, as are interface routes in the IP routing table.

Secondary IP addresses can be used in a variety of situations. The following are the most common applications:

- There may not be enough host addresses for a particular network segment. For example, your subnetting allows up to 254 hosts per logical subnet, but on one physical subnet you need to have 300 host addresses. Using secondary IP addresses on the routers or access servers allows you to have two logical subnets using one physical subnet.
- Many older networks were built using Level 2 bridges. The judicious use of secondary addresses can aid in the transition to a subnetted, router-based network. Routers on an older, bridged segment can be easily made aware that there are many subnets on that segment.

Huawei Command Reference, Version 1.5, Volume 1, Module 04, pp. 1-1 to 1-2

<http://datacomm.huawei.com/english/index.html>

[Select "Document Center" link; then select "VRP Command and Configuration Manual" link; then select "Command Reference V1.5"; then select "Command Reference(V1.5)-Volume 1" link.]

Cisco Network Protocols Command Reference, Part 1, Version 11.2, IP Commands,

pp. V-57 to V-58

http://www.cisco.com/en/US/products/sw/iosswrel/ps1824/products_command_reference_chapter-0918ea00080080d98.html
[Select "ip address" link or select PDF file for entire document and go to cited pages]

Huawei “ip unnumbered” Command (1 of 2)

1.1.4 ip unnumbered

To enable IP processing on a serial interface without assigning an explicit IP address to the interface, use the **ip unnumbered** command. To disable the IP processing on the interface, use the **no** form of this command.

ip unnumbered interface-type interface-number

no ip unnumbered

Syntax Description

interface-type type of another interface on which the router has an assigned IP address.

interface-number number of another interface on which the router has an assigned IP address.

Command Mode

Interface configuration mode

Cisco “ip unnumbered” Command (1 of 2)

Chapter 1

User Manual – Command Reference (Volume 1)
Versatile Routing Platform

* * * *

ip unnumbered

To enable IP processing on a serial interface without assigning an explicit IP address to the interface, use the **ip unnumbered** interface configuration command. To disable the IP processing on the interface, use the **no** form of this command.

ip unnumbered type number
no ip unnumbered type number

Syntax Description

type number

Type and number of another interface on which the router has an assigned IP address. It cannot be another unnumbered interface.

Default

Disabled

Command Mode

Interface configuration

Huawei Command Reference, Version 1.5, Volume 1, Module 04, pp. 1-3 to 1-4
<http://datacomm.huawei.com/english/index.html>

[Select “Document Center” link; then select “VRP Command and Configuration Manual” link; then select “Command Reference V1.5”; then select “Command Reference(V1.5)- Volume 1” link.]

Cisco Network Protocols Command Reference, Part 1, Version 11.2, IP Commands, pp. V-147 to V-148

http://www.cisco.com/en/US/products/sw/iosswrel/ps1824/products_command_reference_chapter09186a0080080d98.html
[Select “ip unnumbered” link, or select PDF icon for entire document and go to cited pages]

Huawei “ip unnumbered” Command (2 of 2)

User Manual – Command Reference (Volume 1)
Versatile Routing Platform
IP Address Configuration Commands

Usage Guideline

Whenever the unnumbered interface generates a packet (for example, for a routing update), it uses the address of the specified interface as the source address of the IP packet. It also uses the address of the specified interface in determining which routing processes are sending updates over the unnumbered interface. Restrictions include the following:

- 1) Serial interfaces using HDLC, PPP, Balanced (LAPB), and Frame Relay encapsulations, as well as Serial Line Internet Protocol (SLIP) and tunnel interfaces can be unnumbered. It is not possible to use this interface configuration command with X.25 or Switched Multimegabit Data Service (SMDS) interfaces.
 - 2) You cannot use the **ping** command to determine whether the interface is up, because the interface has no address. Simple Network Management Protocol (SNMP) can be used to remotely monitor interface status.
 - 3) You cannot netboot a runnable image over an unnumbered serial interface.
 - 4) You cannot support IP security options on an unnumbered interface.
- The interface you specify by the type and number arguments must be enabled (listed as ‘up’ in the **show interfaces** command display).

The **interface-type interface-number** cannot be another unnumbered interface.

Example

! Allow IP unnumbered from Ethernet 0 encapsulated with PPP.

Quidway(config-if-Serial0)# ip unnumbered ethernet 0

Related Command

ip proxy-arp

Huawei Command Reference, Version 1.5, Volume 1, Module 04, pp. 1-3 to 1-4
<http://datacomm.huawei.com/english/index.html>

[Select “Document Center” link; then select “VRP Command and Configuration Manual” link; then select “Command ReferenceV1.5”; then select “Command Reference(V1.5)-Volume 1” link.]

Cisco “ip unnumbered” Command (2 of 2)

ip unnumbered

*** * * ***

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

Whenever the unnumbered interface generates a packet (for example, for a routing update), it uses the source address of the IP packet. It also uses the address of the specified interface as the source address of the IP packet. If also uses the address of the specified interface in determining which routing processes are sending updates over the unnumbered interface. Restrictions include the following:

- Serial interfaces using HDLC, PPP, Link Access Procedure, Balanced (LAPB), and Frame Relay encapsulations, as well as Serial Line Internet Protocol (SLIP) and tunnel interfaces can be unnumbered. It is not possible to use this interface configuration command with X.25 or unnumbered. It is not possible to use this interface configuration command with X.25 or Switched Multimegabit Data Service (SMDS) interfaces.
 - You cannot use the **ping** EXEC command to determine whether the interface is up, because the interface has no address. Simple Network Management Protocol (SNMP) can be used to remotely monitor interface status.
 - You cannot netboot a runnable image over an unnumbered serial interface.
 - You cannot support IP security options on an unnumbered interface.
- The interface you specify by the type and number arguments must be enabled (listed as ‘up’ in the **show interfaces** command display).

The interface you specify by the type and number arguments must be enabled (listed as ‘up’ in the **show interfaces** command display).

If you are configuring IS-IS across a serial line, you should configure the serial interfaces as unnumbered. This allows you to conform with RFC 1195, which states that IP addresses are not required on each interface.

Cisco Network Protocols Command Reference, Part 1, Version 11.2, IP Commands,

pp. V-147 to V-148

http://www.cisco.com/en/US/products/sw/iosswrel/ps1824/products_command_reference_chapter0918ea0080080d98.html

[Select “Document Center” link; then select “VRP Command and Configuration Manual” link; then select “Command ReferenceV1.5”; then select “Command Reference(V1.5)-Volume 1” link, or select PDF icon for entire document and go to cited pages]

Huawei “ip tcp header-compression” Command (1 of 2)

User Manual – Command Reference (Volume 1)
Versatile Routing Platform
IP Performance Configuration Commands

2.7 ip tcp header-compression

To enable TCP header compression, use the **ip tcp header-compression** command.

To disable compression, use the **no** form of this command.

ip tcp header-compression

no ip tcp header-compression

Default

Disabled

Command Mode

Interface configuration mode

Huawei Command Reference, Version 1.5, Volume 1, Module 04, pp. 2-4 to 2-5
<http://datacomm.huawei.com/english/index.html>

[Select “Document Center” link; then select “VRP Command and Configuration Manual” link; then select “Command Reference V1.5”; then select “Command Reference(V1.5)-Volume 1” link.]

Cisco “ip tcp header-compression” Command (1 of 2)

Chapter 2
ip tcp header-compression

ip tcp header-compression

To enable TCP header compression, use the **ip tcp header-compression** interface configuration command. To disable compression, use the **no** form of this command.

ip tcp header-compression [passive]

no ip tcp header-compression [passive]

Syntax Description

passive

(Optional) Compresses outgoing TCP packets only if incoming TCP packets on the same interface are compressed. If you do not specify the **passive** keyword, the Cisco IOS software compresses all traffic.

Default

Disabled

Command Mode

Interface configuration

Cisco Network Protocols Command Reference, Part 1, Version 11.2, IP Commands, pp. V-142
http://www.cisco.com/en/US/products/swiosswrel/ps1824/products_command_reference_chapter09186a0080080d98.html

[Select “ip tcp header-compression” link, or select PDF file for entire document and go to cited page]

Huawei “ip tcp header-compression” Command (2 of 2)

Chapter 2

IP Performance Configuration Commands

User Manual – Command Reference (Volume 1)
Versatile Routing Platform

* * *

Usage Guideline

When running PPP in the lines of low speed WAN, the TCP header accounts for a large proportion in all the transmitting data, so TCP header-compression can be used to improve the efficiency of data transmission.

You can compress the headers of your TCP/IP packets in order to reduce the size of your packets. TCP header compression is supported on serial lines using Frame Relay, HDLC or Point-to-Point (PPP) encapsulation. You must enable compression on both ends of a serial connection. RFC 1144 specifies the compression process. Compressing the TCP header can speed up Telnet connections dramatically. In general, TCP header compression is advantageous when your traffic consists of many small packets, not for traffic that consists of large packets. Transaction processing (usually using terminals) tends to use small packets while file transfers use large packets. This feature only compresses the TCP header, so it has no effect on UDP packets or other protocol headers.

When compression is enabled, fast switching is disabled. This means that fast interfaces like T1 can overload the router. Consider your network's traffic characteristics before using this command.

Example

! Enable TCP header-compression at the PPP interface Serial0.

Quidway(config-if-Serial0)# ip tcp header-compression

Related Command

encapsulation ppp

Huawei Command Reference, Version 1.5, Volume 1, Module 04, pp. 2-4 to 2-5

<http://datacomm.huawei.com/english/index.html>

[Select “Document Center” link; then select “VRP Command and Configuration Manual” link; then select “Command Reference V1.5”; then select “Command Reference(V1.5)-Volume 1” link.]

Cisco “ip tcp header-compression” Command (2 of 2)

Chapter 2

IP Performance Configuration Commands

ip tcp header-compression

* * *

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.B

You can compress the headers of your TCP/IP packets in order to reduce the size of your packets. TCP header compression is supported on serial lines using Frame Relay, HDLC or Point-to-Point (PPP) encapsulation. You must enable compression on both ends of a serial connection. RFC 1144 specifies the compression process. Compressing the TCP header can speed up Telnet connections dramatically. In general, TCP header compression is advantageous when your traffic consists of many small packets, not for traffic that consists of large packets. Transaction processing (usually using terminals) tends to use small packets while file transfers use large packets. This feature only compresses the TCP header, so it has no effect on UDP packets or other protocol headers.

When compression is enabled, fast switching is disabled. This means that fast interfaces like T1 can overload the router. Consider your network's traffic characteristics before using this command.

Example

In the following example, the first serial interface is set for header compression with a maximum of ten cache entries:

```
interface serial 0
  ip tcp header-compression
    ip tcp compression-on-connections 10
```

Related Command

```
ip tcp compression-connections
  ip tcp compression-on-connections
```

Cisco Network Protocols Command Reference, Part 1, Version 11.2, IP Commands,

pp. V-142

http://www.cisco.com/en/US/products/sw/fioswrel/ps1824/products_command_reference_chapter09186a0080080d98.html

[Select “ip tcp header-compression” link, or select PDF file for entire document and go to cited page]

EXHIBIT C

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION**

MOTOROLA, INC.,)	
)	
Plaintiff,)	
v.)	
LEMKO CORPORATION, XIAOHONG)	
SHENG, SHAOWEI PAN, HANJUAN)	
JIN, XIAOHUA WU, XUEFENG BAI,)	
NICHOLAS LABUN, BOHDAN)	
PYSKIR, HECHUN CAI, JINZHONG)	
ZHANG, ANGEL FAVILA, ANKUR)	Case No. 08 CV 5427
SAXENA, RAYMOND HOWELL, FAYE)	
VORICK, NICHOLAS DESAI, and)	
HUAWEI TECHNOLOGIES CO., LTD., a)	
Chinese corporation,)	
)	
Defendants.)	Judge Matthew F. Kennelly
* * * * *)	
LEMKO CORPORATION, SHAOWEI)	Magistrate Judge Geraldine Soat Brown
PAN, XIAOHUA WU and XIAOHONG)	
SHENG,)	
)	
Counter-Plaintiffs,)	
)	
v.)	
MOTOROLA, INC.,)	
)	
Counter-Defendant.)	

THIRD AMENDED COMPLAINT

Plaintiff Motorola, Inc. (“Motorola” or “Plaintiff”), by and through its attorneys, for its Third Amended Complaint against Defendant Lemko Corporation (“Lemko”), Defendant Shaowei Pan (“Pan”), Defendant Hanjuan Jin (“Jin”), Defendant Xiaohua Wu (“Wu”), Defendant Xuefeng Bai (“Bai”), Defendant Xiaohong Sheng (“Sheng”), Defendant Nicholas Labun (“Labun”), Defendant Bohdan Pyskir (“Pyskir”), Defendant Hechun Cai (“Cai”), Defendant Jinzhong Zhang (“Zhang”), Defendant Angel Favila (“Favila”), Defendant Ankur

Saxena (“Saxena”), Defendant Raymond Howell (“Howell”), Defendant Faye Vorick (“Vorick”), Defendant Nicholas Desai (“Desai”), and Defendant Huawei Technologies Co., Ltd. (“Huawei”) (together “Defendants”), alleges and states as follows:

NATURE OF ACTION

1. This is an action for violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, *et. seq.*, for threatened or actual misappropriation of trade secrets arising under the Illinois Trade Secrets Act, 765 ILCS 1065/1 *et seq.*, breach of fiduciary duty, breach of contract, usurpation of corporate opportunity, copyright infringement, declaratory judgment of patent ownership, tortious interference with contract, common law fraud, spoliation of evidence and civil conspiracy.

THE PARTIES

2. Plaintiff Motorola is a corporation organized and existing under the laws of the State of Delaware, with its principal place of business and world headquarters at 1303 East Algonquin Road, Schaumburg, Illinois 60196.

3. Defendant Lemko is a corporation organized and existing under the laws of Illinois, with its principal place of business at 1700 East Golf Road, 7th Floor, Schaumburg, Illinois 60173.

4. Defendant Pan is a citizen of Illinois, domiciled at 21878 North Tall Hills Drive, Kildeer, Illinois 60047, with a business address of 1700 East Golf Road, 7th Floor, Schaumburg, Illinois 60173. Pan is the Chief Technology Officer and Director of Defendant Lemko. Defendant Pan was employed and paid a salary by Motorola from about August 1, 1994 through about April 2, 2004.

5. Defendant Jin is a citizen of Illinois, domiciled at 2331 County Farm Lane, Schaumburg, Illinois 60194-4808. Defendant Jin was employed and paid a salary by

Motorola from 1998 through about February 27, 2007. Motorola employed Jin as a software engineer in its Schaumburg, Illinois offices.

6. Defendant Wu is a citizen of Illinois, domiciled at 21878 North Tall Hills Drive, Kildeer, Illinois 60047. Defendant Wu was employed and paid a salary by Motorola from about June 1995 through about December of 2007. Motorola employed Wu as an engineer at its Schaumburg, Illinois offices. Defendant Wu is the spouse of Defendant Pan.

7. Defendant Bai is a citizen of Illinois, domiciled at 2444 Palazzo Court, Buffalo Grove, Illinois 60089. Defendant Bai was employed and paid a salary by Motorola from about January 2001 through about December of 2007. Motorola employed Bai as a software engineer at its Libertyville, Illinois offices.

8. Defendant Sheng is a citizen of California, domiciled at 4290 Albany Drive, San Jose, California. Sheng was employed and paid a salary by Motorola from about November 2006 through about July of 2008, Motorola employed Sheng as a software engineer at its Libertyville, Illinois offices.

9. Defendant Labun is a citizen of Illinois, domiciled at 1325 North State Parkway, 22F, Chicago, Illinois 60610. Labun is the Chief Executive Officer and Director of Defendant Lemko. Labun was employed and paid a salary by Motorola from September 25, 1989 through about May 10, 2004. Labun was Vice President of Business Development at Motorola.

10. Defendant Pyskir is a citizen of Illinois, domiciled at 645 Chesterfield Avenue, Naperville, Illinois 60540. Pyskir is the President and Director of Defendant Lemko. Pyskir was employed and paid a salary by Motorola from about January 7, 1993 through about March 31, 2004. Defendant Pyskir was a senior director within Motorola's management team.

11. Defendant Cai is a citizen of Illinois, domiciled at 1254 South Falcon Drive, Palatine, Illinois 60067. Cai is currently employed by Defendant Lemko as a software engineer. Cai was employed and paid a salary by Motorola from about October 26, 1998 through about May 19, 2005. Motorola employed Cai as a software engineer.

12. Defendant Zhang is a citizen of Illinois, domiciled at 1119 Berkshire Lane, Barrington, Illinois 60010. Zhang is currently employed by Defendant Lemko. Zhang was employed and paid a salary by Motorola from about May 19, 1995 through about July 11, 2004. Motorola employed Zhang as a software engineer.

13. Defendant Favila is a citizen of Illinois, domiciled at 5419 Crossview Lane, Lake In The Hills, Illinois 60156. Favila was employed and paid a salary by Motorola from about December 18, 1989 through the present. Motorola employed Favila as a software engineer.

14. Defendant Saxena is a citizen of Illinois, domiciled at 1043 North Glenview Court, Palatine, Illinois 60067. Saxena is currently employed by Defendant Lemko as a software engineer. Saxena was employed and paid a salary by Motorola from about May 31, 2000 through about August 2, 2005. Motorola employed Saxena as a software engineer.

15. Defendant Howell is a citizen of Illinois, domiciled at 26680 North Countryside Lake Drive, Mundelein, Illinois 60060. Howell was the Chief Financial Officer and Director of Defendant Lemko until about November 2008. Howell was employed by Motorola from about September 28, 1981 through about October 30, 1998. Motorola employed Howell as a Director of Finance.

16. Defendant Vorick is a citizen of Illinois, domiciled at 425 West Parkside Drive, Palatine, Illinois 60067. Vorick is the VP of Marketing for Defendant Lemko. Vorick was

employed by Motorola from about June 19, 1989 through about September 6, 2001. Motorola employed Vorick as a Senior Marketing Manager.

17. Defendant Desai is a citizen of California, domiciled at 1915 Mathews #2, Redondo Beach, CA 90278. Desai is the VP Business Development for Defendant Lemko.

17.1 Defendant Huawei is a foreign corporation with its principal place of business in Shenzhen, People's Republic of China. Defendant Huawei is a global vendor and provider of telecommunications services.

JURISDICTION AND VENUE

18. This Court has subject matter jurisdiction over Plaintiff's claims arising under the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030, *et seq.*, pursuant to 28 U.S.C. § 1331. This Court also has supplemental jurisdiction over all other claims asserted herein pursuant to 28 U.S.C. § 1337 because those claims are so related to the claims brought under the CFAA so as to form part of the same case or controversy.

19. This Court has personal jurisdiction over Defendant Lemko. Defendant Lemko is registered to do business in the State of Illinois. Defendant Lemko also has a regular and established place of business in Illinois and this District at 1700 East Golf Road, Schaumburg, Illinois 60173, and is and has been doing business in Illinois and this District at all times relevant hereto.

20. This Court has personal jurisdiction over Defendant Pan. On information and belief, at all times relevant hereto, Defendant Pan has resided in Illinois and in the District, has acted as an officer of Defendant Lemko, and/or has committed tortious acts in Illinois and this District. Defendant Pan's wrongful conduct, as set forth herein, arises out of and is related to the business he has transacted and the tortious acts he has committed in this State and District.

21. This Court has personal jurisdiction over Defendant Jin. On information and belief, at all times relevant hereto, Defendant Jin has resided in Illinois and in this District, has transacted business with Defendant Lemko in this District, and/or has committed tortious acts in Illinois and this District. Defendant Jin's wrongful conduct, as set forth herein, arises out of and is related to the business she has transacted and the tortious acts she has committed in this State and District.

22. This Court has personal jurisdiction over Defendant Wu. On information and belief, at all times relevant hereto, Defendant Wu has resided in Illinois and in this District, has transacted business with Defendant Lemko in this District, and/or has committed tortious acts in Illinois and this District. Defendant Wu's wrongful conduct, as set forth herein, arises out of and is related to the business she has transacted and the tortious acts she has committed in this State and District.

23. This Court has personal jurisdiction over Defendant Bai. On information and belief, at all times relevant hereto, Defendant Bai has resided in Illinois and in this District, has transacted business with Defendant Lemko in this District, and/or has committed tortious acts in Illinois and this District. Defendant Bai's wrongful conduct, as set forth herein, arises out of and is related to the business he has transacted and the tortious acts he has committed in this State and District.

24. This Court has personal jurisdiction over Defendant Sheng. On information and belief, at all times relevant hereto, Defendant Sheng resided in Illinois and in this District, has transacted business with Defendant Lemko in this District, and/or has committed tortious acts in Illinois and this District. Defendant Sheng's wrongful conduct, as set forth herein, arises out

of and is related to the business she has transacted and the tortious acts she has committed in this State and District.

25. This Court has personal jurisdiction over Defendant Labun. On information and belief, at all times relevant hereto, Defendant Labun has resided in Illinois and in this District, has transacted business with Defendant Lemko in this District, and/or has committed tortious acts in Illinois and this District. Defendant Labun's wrongful conduct, as set forth herein, arises out of and is related to the business he has transacted and the tortious acts he has committed in this State and District.

26. This Court has personal jurisdiction over Defendant Pyskir. On information and belief, at all times relevant hereto, Defendant Pyskir has resided in Illinois and in this District, has transacted business with Defendant Lemko in this District, and/or has committed tortious acts in Illinois and this District. Defendant Pyskir's wrongful conduct, as set forth herein, arises out of and is related to the business he has transacted and the tortious acts he has committed in this State and District.

27. This Court has personal jurisdiction over Defendant Cai. On information and belief, at all times relevant hereto, Defendant Cai has resided in Illinois and in this District, has transacted business with Defendant Lemko in this District, and/or has committed tortious acts in Illinois and this District. Defendant Cai's wrongful conduct, as set forth herein, arises out of and is related to the business he has transacted and the tortious acts he has committed in this State and District.

28. This Court has personal jurisdiction over Defendant Zhang. On information and belief, at all times relevant hereto, Defendant Zhang has resided in Illinois and in this District, has transacted business with Defendant Lemko in this District, and/or has committed

tortious acts in Illinois and this District. Defendant Zhang's wrongful conduct, as set forth herein, arises out of and is related to the business he has transacted and the tortious acts he has committed in this State and District.

29. This Court has personal jurisdiction over Defendant Favila. On information and belief, at all times relevant hereto, Defendant Favila has resided in Illinois and in this District, has transacted business with Defendant Lemko in this District, and/or has committed tortious acts in Illinois and this District. Defendant Favila's wrongful conduct, as set forth herein, arises out of and is related to the business he has transacted and the tortious acts he has committed in this State and District.

30. This Court has personal jurisdiction over Defendant Saxena. On information and belief, at all times relevant hereto, Defendant Saxena has resided in Illinois and in this District, has transacted business with Defendant Lemko in this District, and/or has committed tortious acts in Illinois and this District. Defendant Saxena's wrongful conduct, as set forth herein, arises out of and is related to the business he has transacted and the tortious acts he has committed in this State and District.

31. This Court has personal jurisdiction over Defendant Howell. On information and belief, at all times relevant hereto, Defendant Howell has resided in Illinois and in this District, has transacted business with Defendant Lemko in this District, and/or has committed tortious acts in Illinois and this District. Defendant Howell's wrongful conduct, as set forth herein, arises out of and is related to the business he has transacted and the tortious acts he has committed in this State and District.

32. This Court has personal jurisdiction over Defendant Vorick. On information and belief, at all times relevant hereto, Defendant Vorick has resided in Illinois and in this

District, has transacted business with Defendant Lemko in this District, and/or has committed tortious acts in Illinois and this District. Defendant Vorick's wrongful conduct, as set forth herein, arises out of and is related to the business she has transacted and the tortious acts she has committed in this State and District.

33. This Court has personal jurisdiction over Defendant Desai. On information and belief, at all times relevant hereto, Defendant Desai has transacted business with Defendant Lemko in this District, and/or has committed tortious acts in Illinois and this District. Defendant Desai's wrongful conduct, as set forth herein, arises out of and is related to the business he has transacted and the tortious acts he has committed in this State and District.

33.1 This Court has personal jurisdiction over Defendant Huawei. On information and belief, at all times relevant hereto, Defendant Huawei has transacted business with Defendant Lemko in this District, and/or has committed tortious acts in Illinois and this District. Defendant Huawei also has a regular and established place of business in Illinois at 3601 Algonquin Road, Rolling Meadows, IL 60008 and, on information and belief, has been doing business in Illinois and this District at all times relevant hereto. Defendant Huawei's wrongful conduct, as set forth herein, arises out of and is related to the business it has transacted and the tortious acts it has committed in this State and District.

34. Venue is proper in this judicial district pursuant to 28 U.S.C. §§ 1391(b) and (c).

GENERAL ALLEGATIONS

35. Motorola is a global leader in communications technologies. For nearly 80 years, Motorola has competed at the forefront of research and development of communication technologies, products and services.

36. Motorola is recognized worldwide for its innovations in communications including, without limitation, enterprise mobility solutions, cellular infrastructure systems,

mission-critical communication tools, emergency and disaster relief communication tools, home and network communications and mobile devices.

Motorola's Proprietary Communications Technologies

37. Motorola's proprietary and confidential mobile communications technologies include: proprietary cellular service and product technologies; proprietary wireless broadband and wireless access service and product technologies; proprietary voice communications service and product technologies; proprietary data communications service and product technologies; proprietary integrated voice and data communication systems technologies; proprietary radio systems technologies; proprietary integrated emergency-response communications systems, service, and product technologies; proprietary integrated radio, wireless broadband, voice, and/or data communications systems, service, and product technologies; proprietary communications designs, solutions, initiatives, and equipment; proprietary iDen technology; proprietary information dispatch and networking technology; proprietary Push-to-Talk technology; proprietary ICD technology; proprietary WiMax technology; proprietary SATCOW technology; proprietary SIP-related technology; proprietary subsidy unlock codes; proprietary global system for mobile communication ("GSM") development tools and data; proprietary Universal Mobile Telecommunications System ("UMTS") technology; proprietary W-CDMA technology; proprietary "log files" recording the specific functions of Motorola telephones; proprietary "dump file" software files; proprietary Motorola virtual private network ("VPN") access software; and proprietary and unique confidential combinations and compilations of the above information (hereinafter referred to in the aggregate as "Motorola's proprietary trade secrets and confidential information").

38. Motorola's proprietary trade secrets and confidential information are not generally known in the trade, and Motorola derives economic value and a competitive advantage

in the marketplace from the secrecy of such information. Indeed, Motorola's proprietary trade secrets and confidential information are Motorola's lifeblood as a technology leader whose market position depends upon its innovations.

39. Motorola has invested hundreds of millions of dollars, many times over, researching and developing its proprietary trade secrets and confidential information.

40. At all times relevant hereto, Motorola has used reasonable measures to protect the secrecy of its proprietary trade secrets and confidential information, including but not limited to: restricted access on a need-to-know basis; global confidentiality policies; contractual confidentiality restrictions; security key cards; password-protected computer and network platforms; and a wide array of additional physical security measures.

41. For example, Motorola has, at all times relevant hereto, required its engineers to sign confidentiality agreements. One such employment agreement reads in part:

In consideration of my employment, or continued employment by Motorola, Inc. . . . and the salary or wages paid to me, I understand and agree to the following provisions for the protection of Motorola property rights:

1. Not to disclose to Motorola, or to use in my work at Motorola (a) any confidential information belonging to others, including my prior employers . . . or (b) any prior inventions made by me which Motorola is not otherwise entitled to learn of or to use.
2. Not to use, or to publish, or to otherwise disclose to others, either during or subsequent to my employment by Motorola, any confidential information of Motorola . . . , except as my Motorola duties may require.
3. Upon my termination of my employment by Motorola, to promptly deliver to a designated Motorola representative all documents and other records which are related to the business activities of Motorola, or any other materials which belong to Motorola.
4. To assign and I hereby assign to Motorola as its exclusive property the entire right, title and interest in all my inventions, innovations, or ideas developed or conceived by me solely, or jointly with others, at any time during the term of my employment and which inventions, innovations, or ideas relate to the actual or anticipated business activities of Motorola, or result from, or are suggested by, work which I do for Motorola.

...
(EXHIBIT A.)

42. Also, since at least 2006, Motorola has required its engineers to sign an "Employment Confidentiality and Assignment of Inventions Agreement," which reads in part:

1. Nondisclosure of Confidential Information

Definitions: As used in this Agreement, "Confidential Information" means all confidential information and trade secrets (whether or not specifically labeled or identified as "confidential"), in any form or medium, that is disclosed to, or developed or learned by me and that relates to the business, products, services, research or development of Motorola or its suppliers, distributors or customers and that has not become publicly known.

...
I recognize that Motorola is engaged in a continuous program of research and development, and that as an employee, I will have access to Confidential Information that has independent economic value to Motorola in part because it is confidential. I further recognize that Motorola has taken reasonable steps to protect its Confidential Information from disclosure to the public, including entering into this Agreement. During and after my employment, I will not disclose or use any Confidential Information except to the extent I am required to disclose or use such Confidential Information in the performance of my assigned duties; and I will use my best efforts to safeguard the Confidential Information and protect it against disclosure, misuse, espionage, loss and theft.

...
3. Ownership and Return of Materials

All documents and materials, which I have had access to or produced in connection with my services for Motorola, or which belong to Motorola, whether or not such materials contain Confidential Information, shall remain the sole property of Motorola. Upon termination, or at any time requested, I shall promptly deliver to Motorola all such materials and copies in my possession and control and shall provide written confirmation that I have returned all such materials.

...
5. Noncompliance

...
I acknowledge that my compliance with this Agreement is necessary to protect Motorola's goodwill and Confidential Information, that my failure to comply with this Agreement will irreparably harm the business of Motorola, and that monetary damages would not provide an adequate remedy to Motorola in the event of such non-compliance. Therefore, Motorola shall be entitled to obtain an injunction and other equitable relief in any court of competent jurisdiction against a breach by me of this Agreement.

(EXHIBIT B.)

43. Motorola maintains strict policies over its employees' use of its information assets (including any information, tangible or intangible, physical or digital, that is owned or created

by Motorola, or is entrusted to Motorola by a third party) and information resources (including technology hardware such as computers, servers, personal digital assistants, telephones, networks, routers, accessories, storage media, and the software supporting the hardware such as operating systems, databases, and applications such as e-mail, and services) owned by, leased to, or otherwise operated by Motorola.

44. These policies have been codified in part in Motorola policies governing the appropriate use of computer resources and protection of proprietary information. For example, Motorola's "Protection of Proprietary Information" policy provides that

"Each employee has a responsibility not to use, or to publish, or to otherwise disclose to others, any proprietary or confidential information of Motorola or its customers or suppliers or other contractors, except as Motorola duties may require. Each employee should report information security breaches to the Corporate Security Department and the local Security Department."

45. Additionally, Motorola's "Information Protection Policy and Control Standards for Information Users" ("iProtect") policy prohibits "inappropriate use of Motorola's Information Resources," including, without limitation:

"Disclosing information that is owned by Motorola, or entrusted by a third party to Motorola, to unauthorized recipients;"

"Enabling non-Motorolans who have not signed the proper non-disclosure agreements with Motorola to access a Motorola provided network connection;"

"Misusing intellectual property (e.g., trademarks, copyrights, or patents) of Motorola or a third party;" and

"Accessing Motorola Confidential Restricted and similar non-Motorola information on Information Resources without authorization."

46. The iProtect policy also provides that "User IDs must not be utilized by anyone except the individual to whom the IDs have been issued. Users are responsible for all activity performed with their User IDs." Finally, it provides that "Motorola Confidential Restricted

information, Internal information, and Third Party Proprietary Information may not be removed or sent from Motorola's premises unless there is a business requirement to do so."

47. Motorola also requires its employees to adhere to the Motorola "Code of Business Conduct" (previously titled the Motorola "Code of Conduct") that instructs employees:

We may not work for or receive payments for services from any competitor, customer, distributor or supplier of Motorola without prior approval. Any outside activity must be strictly separated from Motorola employment and should not harm job performance at Motorola. Skills learned and used at Motorola must not be used in a way that could hurt the business of Motorola.

Defendants Lemko and Jin Conspire to Smuggle Motorola's Trade Secrets and Other Proprietary Motorola Documents to China

48. In 1998, Motorola employed Defendant Jin as a software engineer, where she remained employed for the next nine years, until February of 2007. Defendant Jin is a naturalized U.S. citizen and a citizen of the People's Republic of China by birth.

49. Defendant Lemko is a privately held company headquartered in Schaumburg, Illinois with additional offices in China and India.

50. Defendant Lemko is Motorola's direct competitor in areas such as the development and marketing of cellular infrastructure systems, cellular voice, high-speed data and text services, emergency and disaster relief communication systems, wireless communication and control applications for government markets, and rural cellular solutions. Defendant Lemko advertises itself with the trademark "Wireless for the Next Billion People."

51. In the course of her employment as a software engineer with Motorola, Defendant Jin had access to Motorola's proprietary trade secrets and confidential information in the performance of her duties.

52. Motorola reposed a high level of trust and confidence in Defendant Jin's trustworthiness, integrity, and fidelity to her obligations towards Motorola. These duties were

memorialized in part through Jin's executed "Employee Agreement" and her signed acknowledgment of Motorola's Code of Conduct.

53. In or before June of 2004, without Motorola's knowledge or consent, Defendant Jin accepted employment with Defendant Lemko. Defendant Jin continued her employment with Motorola until February of 2007, but never disclosed her simultaneous employment with Defendant Lemko to Motorola, in violation of the Motorola "Code of Business Conduct," which provided that employees "may not work for or receive payments for services from any competitor, customer, distributor or supplier of Motorola without prior approval," and required employees to "disclose any situation that may be or appear to be a conflict of interest."

54. On March 24, 2005, shortly after accepting employment with Defendant Lemko, Defendant Jin intentionally, knowingly, with intent to defraud, accessed Motorola's protected computers and obtained and transferred by e-mail, in furtherance of that fraud, valuable Motorola proprietary trade secrets and confidential information, including Motorola source code, from Motorola's protected computers to her non-secure personal e-mail account without authorization or exceeding her authorized access, without Motorola's knowledge or consent, and in violation of Motorola's confidentiality and security policies, thereby knowingly and recklessly causing damage and loss by impairing the integrity and/or availability of the Motorola proprietary trade secrets and confidential information and the Motorola protected computers.

55. Beginning in or before June of 2005, Defendant Jin intentionally, knowingly, and with the intent to defraud, accessed her Lemko webmail account through the secure Motorola network of protected Motorola computers, without authorization or exceeding her authorized access, and without Motorola's knowledge or consent.

56. Between June 15, 2005 and September 1, 2005, Defendant Jin took a partial leave of absence, during which time Defendant Jin was still a Motorola employee but did not report to work at Motorola full time. Defendant Jin also continued to work for Defendant Lemko during this period, without Motorola's knowledge or consent.

57. From February of 2006 until February of 2007, Defendant Jin took a prolonged leave of absence from her duties at Motorola, allegedly for medical reasons. During this prolonged leave of absence, Defendant Jin was still a Motorola employee. Again, Defendant Jin continued to work for Defendant Lemko during this medical leave.

58. Even though Defendant Jin had no assigned duties for Motorola during this leave, and even though she was actively working for Defendant Lemko during this time in violation of Motorola's policies, Defendant Jin continued to intentionally and knowingly, and with the intent to defraud, access Motorola's protected computers and its proprietary trade secrets and confidential information through Motorola's secure internal document access system, including, without limitation, documents related to System Architecture Design ("SAD"), ICD technology specifications, Push-to-Talk technology, iDen technology, and WiMax technology, without authorization or exceeding her authorized access, and without Motorola's knowledge or consent. In furtherance of that fraud, Defendant Jin obtained valuable Motorola proprietary trade secrets and confidential information from Motorola's protected computers and recklessly caused damage and loss by impairing their integrity and/or availability.

59. Beginning in February of 2006 or earlier, Defendant Jin installed Motorola's proprietary secure virtual private network ("VPN") access software on non-Motorola computers, including a Lemko-owned computer, intentionally, knowingly, and with an intent to defraud, without authorization or exceeding her authorized access, and without Motorola's knowledge or

consent. During her period of leave, Defendant Jin frequently accessed Motorola's protected computers through Motorola's secure VPN from these non-Motorola computers, including a Lemko-owned computer, without authorization or exceeding her authorized access, and without Motorola's knowledge or consent. By accessing Motorola's protected computers from a Lemko-owned computer in this manner, Defendant Jin, in furtherance of that fraud, obtained valuable information from Motorola's protected computers and recklessly caused damage and loss by impairing the integrity and/or availability of the Motorola proprietary trade secrets and confidential information and the Motorola protected computers.

60. In February of 2007, while still on medical leave from Motorola, Defendant Jin travelled to China, returning on February 15, 2007. While she was in China, Defendant Jin obtained access to Motorola's protected computers through Motorola's secure VPN on multiple occasions, intentionally, knowingly, and with an intent to defraud, without authorization or exceeding her authorized access, and without Motorola's knowledge or consent. By accessing Motorola's protected computers in this manner, Defendant Jin, in furtherance of that fraud, obtained valuable information from Motorola's protected computers and recklessly caused damage and loss by impairing the integrity and/or availability of the Motorola proprietary trade secrets and confidential information and the Motorola protected computers.

61. Between February 18 and 19, 2007, Defendant Jin continued to access Motorola's proprietary trade secrets and confidential information from Motorola's protected computers through Motorola's secure internal document access system, intentionally, knowingly, and with an intent to defraud, without authorization or exceeding her authorized access, and without Motorola's knowledge or consent. Defendant Jin, in furtherance of that fraud, obtained valuable information from Motorola's protected computers and recklessly caused damage and loss by

impairing the integrity and availability of the Motorola proprietary trade secrets and confidential information and the Motorola protected computers.

62. On February 23, 2007, Defendant Jin advised Motorola that she was ready to end her leave and return to work for Motorola. Defendant Jin did not advise Motorola at this or at any other time that she had been working secretly for Defendant Lemko since at least 2004.

63. On February 24, 2007, Defendant Jin purchased a one-way ticket to Beijing, China for a flight scheduled to depart on February 28, 2007.

64. On February 26, 2007, Defendant Jin returned to work at Motorola, where she received no work assignments. On that day, without authorization or exceeding her authorized access, and without Motorola's knowledge or consent, Defendant Jin intentionally, knowingly, and with the intent to defraud, accessed Motorola's protected computers and downloaded hundreds of valuable, proprietary and confidential Motorola documents and technical specifications without Motorola's knowledge or consent. Defendant Jin, in furtherance of that fraud, obtained valuable information from Motorola's protected computers and recklessly caused damage and loss by impairing the integrity and/or availability of the Motorola proprietary trade secrets and confidential information and the Motorola protected computers.

65. On the evening of February 26, 2007, Defendant Jin returned to the Motorola offices at approximately 9 p.m. At approximately 9:10 p.m., Defendant Jin accessed Defendant Lemko's webmail system. Defendant Jin then intentionally, knowingly, and with intent to defraud, accessed Motorola's protected computers without authorization or exceeding her authorized access, and without Motorola's knowledge or consent. In furtherance of that fraud, Defendant Jin downloaded additional valuable, proprietary and confidential Motorola documents and recklessly caused damage and loss by impairing the integrity and/or availability of the

Motorola proprietary trade secrets and confidential information and the Motorola protected computers.

66. Around midnight, Defendant Jin intentionally, knowingly, and with intent to defraud, removed, in furtherance of that fraud, numerous valuable, proprietary printed documents and other materials from Motorola's secure offices without authorization or exceeding her authorized access, and without Motorola's knowledge or consent and recklessly caused damage and loss by impairing the integrity and/or availability of the Motorola proprietary trade secrets and confidential information and the Motorola protected computers.

67. On February 27, 2007, at approximately 12:15 p.m., Defendant Jin sent an e-mail to her supervisor at Motorola stating that she was not able to work. Defendant Jin's manager was unable to locate her that afternoon, and was not able to discuss this e-mail with Defendant Jin. Defendant Jin then surreptitiously returned to the Motorola offices at approximately 10:30 p.m. that same night and, as she had the previous night, first logged onto Defendant Lemko's webmail system. Defendant Jin then intentionally, knowingly, and with intent to defraud, accessed Motorola's protected computers and, in furtherance of that fraud, downloaded numerous valuable, proprietary and confidential Motorola documents and technical specifications without authorization or exceeding her authorized access, and without Motorola's knowledge or consent and recklessly caused damage and loss by impairing the integrity and/or availability of the Motorola proprietary trade secrets and confidential information and the Motorola protected computers.

68. On February 28, 2007, while attempting to board a flight to Beijing, China at Chicago's O'Hare International Airport, with over \$30,000 dollars in cash, Defendant Jin was thwarted by U.S. Customs officials, who seized more than 1,000 electronic and paper documents

identified as the property of Motorola, including valuable, proprietary information and trade secrets, in Defendant Jin's possession, including a laptop computer, external hard drives, and a thumb drive.

69. Many of the seized documents were marked as Motorola's confidential property, including detailed schematics relating to Motorola's interstate communication network, architecture and network support information, and documents relating to Motorola's proprietary iDen technology, and Motorola's proprietary SATCOW technology. If the Motorola proprietary trade secrets and confidential information found in Defendant Jin's possession were replicated by a competitor, Motorola would suffer many millions of dollars in harm.

70. To date, Motorola has incurred substantial losses, in excess of \$5,000 in a one-year period, due to Defendant Jin's and Defendant Lemko's unauthorized access to Motorola's protected computers and unauthorized removal, possession, and impairment of Motorola's electronic files and documents, including, without limitation, the costs of investigating Defendant Jin's and Defendant Lemko's actions and assessing the damage they caused.

71. Defendant Jin, individually and in concert with Defendant Lemko, without authorization or exceeding her authorized access, and without Motorola's knowledge or consent, intentionally, knowingly, and with intent to defraud accessed Motorola's protected computers and, in furtherance of that fraud, downloaded, uploaded and transferred valuable Motorola proprietary trade secrets and confidential information for her own benefit and the benefit of others, including Defendant Lemko, by and through nonsecure means into a nonsecure environment, thereby impairing the integrity and/or availability of such information.

72. In April 2008, Defendant Jin was indicted by a Grand Jury sitting in the United States District Court, Northern District of Illinois, for three counts of violation of 18 U.S.C. § 1832(a)(3) relating to Jin's possession of Motorola proprietary documents containing proprietary trade secrets and confidential information. In December 2008, the grand jury brought a six count superseding indictment containing three additional counts alleging violation of 18 U.S.C. § 1831(a)(3) for Jin's possession of Motorola proprietary documents intending and knowing that the offense would benefit a foreign government, namely the People's Republic of China.

**Defendants Wu and Bai's Unauthorized Transfers of Information to
Defendants Pan and Lemko**

73. In June of 1995, Motorola hired Defendant Wu as a staff engineer. Motorola promoted Defendant Wu to more senior engineering positions in 1997 and 1999.

74. Defendant Wu is married to Defendant Pan, who is the current Chief Technology Officer of Defendant Lemko.

75. In July of 1994, Motorola hired Defendant Pan as a staff engineer. Motorola promoted Defendant Pan to the position of senior staff engineer in 1995, and to the position of principal staff engineer in 1996.

76. Defendant Pan resigned from his employment with Motorola in March of 2004.

77. Defendant Bai is a citizen of China and has been studying or working in the United States as an engineer since approximately 1998. In January of 2001, Motorola hired Defendant Bai as a software engineer. In 2002, Motorola promoted Bai to the position of senior software engineer.

78. In the course of their employment as engineers for Motorola, Defendants Wu, Bai, and Pan had access to Motorola's proprietary trade secrets and confidential information in the performance of their duties.

79. Motorola reposed a high level of trust and confidence in the trustworthiness and integrity of Defendants Wu, Bai, and Pan, and in their fidelity to their obligations towards Motorola. These duties were memorialized in part through these Defendants' signed "Employee Agreements" and through their signed acknowledgments of Motorola's "Code of Business Conduct."

80. In the 2005 calendar year, Defendant Wu, on behalf of Defendant Pan, purchased at least 24 Motorola telephones from Motorola's on-line employee store. Motorola policies prohibit employees from purchasing more than four such telephones per calendar year, and prohibit any commercial resale or use of such telephones. Defendant Wu forwarded confirmation of orders placed through her Motorola e-mail address to Defendant Pan's personal e-mail address.

81. On October 8, 2005, Defendant Bai intentionally, knowingly, and with intent to defraud, accessed Motorola's protected computers and, in furtherance of that fraud, obtained and transferred by e-mail three of Motorola's proprietary and confidential subsidy unlock codes to Defendant Wu, without authorization or exceeding his authorized access, and without Motorola's knowledge or consent. Subsidy unlock codes allow individual cellular telephones to interface with multiple carrier systems rather than only with one designated carrier system, and Motorola strictly controls access to these valuable codes. On October 10, 2005, without authorization or exceeding her authorized access, and without Motorola's knowledge or consent, Defendant Wu intentionally, knowingly, and with intent to defraud, accessed Motorola's protected computers

and, in furtherance of that fraud, obtained and forwarded Defendant Bai's October 8 e-mail containing these proprietary and confidential subsidy unlock codes from a protected Motorola computer to Defendant Pan's Lemko e-mail account and personal e-mail account, thereby impairing the integrity and/or availability of these codes.

82. On April 17, 2006, Defendant Pan, using his Lemko e-mail account, sent Defendant Bai a request for another valuable, confidential, proprietary subsidy unlock code for a Motorola telephone. In that same e-mail Defendant Pan also asked Defendant Bai for two specific, highly valuable, confidential and proprietary Motorola development files related to "GSM" telephone technology, including GSM phone "flex" software and a debug tool for reading "GSM send/receive messages." Defendant Pan wrote from his Lemko e-mail account that "[w]e need to find one for the GSM network system development." Defendant Pan also sent a copy of this e-mail to Defendant Wu.

83. That same day Defendant Bai responded to Defendant Pan's request by intentionally, knowingly, and with intent to defraud, accessing Motorola's protected computers and, in furtherance of that fraud, obtaining and sending the valuable, confidential, proprietary Motorola unlock code that Defendant Pan had requested to Pan's Lemko e-mail account from protected Motorola computers, without authorization or exceeding his authorized access, and without Motorola's knowledge or consent. Defendant Bai also stated in this e-mail that he would call Defendant Pan later concerning the requested "debug tool." Defendant Bai sent a copy of this e-mail to Defendant Wu's Motorola e-mail account, who forwarded it to Defendant Pan's personal e-mail account.

84. On August 2, 2006, Defendant Pan wrote Defendant Bai an e-mail from his Lemko e-mail account, asking Defendant Bai for “dump files” relating to W-CDMA technology. Defendant Pan sent a copy of this e-mail to Defendant Wu.

85. “Dump files” are highly valuable, confidential software files that allow a specific cellular telephone’s “log file” to be examined and deciphered. Log files give detailed information about all of the functions and actions of the software and hardware in a cellular telephone. Motorola engineers combine these tools in the course of their GSM development efforts with proprietary Motorola GSM/UMTS software. Motorola “dump files,” the “log files” they decode, and the GSM/UMTS software used to combine them constitute Motorola proprietary trade secrets and confidential information.

86. On September 1, 2006, without authorization or exceeding his authorized access, and without Motorola’s knowledge or consent, Defendant Bai complied with Defendant Pan’s request to share confidential and proprietary Motorola trade secrets by intentionally, knowingly, and with intent to defraud accessing Motorola’s protected computers and, in furtherance of that fraud, obtaining and placing two valuable, confidential, and proprietary Motorola “log files” and a valuable, confidential, and proprietary “dump file” on Motorola’s secure internal document sharing system and recklessly causing damage and loss by impairing the integrity and/or availability of the Motorola proprietary trade secrets and confidential information and the Motorola protected computers. Defendant Bai, in furtherance of the same fraud, then obtained and e-mailed links giving Defendant Pan access to that confidential, proprietary Motorola information to Defendant Pan’s Lemko e-mail account from a protected Motorola computer, in direct violation of Motorola’s information protection and security policies. Defendant Bai sent a copy of this e-mail to Defendant Wu.

87. Between September 4, 2006 and April 24, 2007, an unidentified user accessed the three valuable, confidential proprietary, Motorola files to which Defendant Bai had provided Defendants Pan and Wu access links. One “log file” was accessed once, on September 4, 2006, while the other “log file” and the “dump file” were accessed multiple times, the last access occurring on April 24, 2007.

88. On October 5, 2006, Defendant Pan wrote to Defendant Bai from his Lemko account and confirmed “[w]e loaded your dump file.” Defendant Pan then asked for another valuable, confidential, and proprietary Motorola “dump file” showing the “MAC and RLC layer,” copying the message to Defendant Wu. By these actions, Defendants Pan and Lemko intentionally, knowingly, with intent to defraud, and in furtherance of that fraud requested, accessed, and/or uploaded valuable, confidential and proprietary Motorola information, without authorization, from protected Motorola computers and recklessly caused damage and loss by impairing the integrity and/or availability of the Motorola proprietary trade secrets and confidential information and the Motorola protected computers.

89. On October 21, 2006, Defendant Wu intentionally, knowingly, and with intent to defraud accessed Motorola’s protected computers and, in furtherance of that fraud, obtained and installed Motorola’s highly valuable, confidential, and proprietary GSM/UMTS software, which is used to combine Motorola’s proprietary “log files” and “dump files” for GSM development, onto a Lemko-owned computer without authorization or exceeding her authorized access, and without Motorola’s knowledge or consent and recklessly caused damage and loss by impairing the integrity and/or availability of the Motorola proprietary trade secrets and confidential information and the Motorola protected computers.

90. Defendant Wu has also transferred a considerable number of other Motorola proprietary trade secrets and confidential information to Defendants Pan and Lemko without authorization or exceeding her authorized access, and without Motorola's knowledge or consent. For example, in 2006 or sooner, Defendant Wu intentionally, knowingly, and with intent to defraud accessed Motorola's protected computers and, in furtherance of that fraud, obtained and installed Motorola's proprietary VPN access software on non-Motorola computers, including a Lemko-owned computer, without authorization or exceeding her authorized access, and without Motorola's knowledge or consent. Throughout 2006, without authorization or exceeding her authorized access, and without Motorola's knowledge or consent, Defendant Wu intentionally, knowingly, and with intent to defraud accessed Motorola's protected computers through Motorola's secure VPN, and, in furtherance of that fraud, obtained valuable information on numerous occasions both from a Lemko-owned computer and from a personal computer owned by her husband, Defendant Pan, recklessly causing damage and loss by impairing the integrity and/or availability of the Motorola proprietary trade secrets and confidential information and the Motorola protected computers.

91. On December 1, 2006, in violation of Motorola's information protection and security policies and in excess of her authorization, Defendant Wu intentionally, knowingly, with intent to defraud, and in furtherance of that fraud, gave Defendant Pan access to valuable Motorola proprietary trade secrets and confidential information by e-mailing this information to Defendant Pan's personal e-mail account, copying both her Motorola and her personal email accounts and recklessly caused damage and loss by impairing the integrity and/or availability of the Motorola proprietary trade secrets and confidential information and the Motorola protected computers.

92. On May 31, 2007, without authorization or exceeding her authorized access, and without Motorola's knowledge or consent, Defendant Wu intentionally, knowingly, and with intent to defraud accessed Motorola's protected computers and, in furtherance of that fraud, obtained and e-mailed documents containing valuable Motorola proprietary trade secrets and confidential information relating to passive subscriber location in UMTS technology from a protected Motorola computer to Defendant Pan's personal e-mail account, and recklessly caused damage and loss by impairing the integrity and/or availability of the Motorola proprietary trade secrets and confidential information and the Motorola protected computers.

93. In December of 2007, Motorola terminated Defendant Wu's and Defendant Bai's employment for violations of the Motorola policies.

94. To date, Motorola has incurred substantial losses, in excess of \$5,000 in a one-year period, due to Defendant Wu's, Defendant Bai's, Defendant Pan's, and Defendant Lemko's unauthorized access to Motorola's protected computers and unauthorized removal, possession, and impairment of Motorola's electronic files and documents, including without limitation the costs of investigating these Defendants' actions and assessing the damage they caused.

95. Defendants Wu, Bai, Pan, and Lemko, individually and in concert, without authorization or exceeding their authorized access, and without Motorola's knowledge or consent, intentionally, knowingly, and with intent to defraud accessed Motorola's protected computers, and, in furtherance of that fraud, downloaded, uploaded and transferred Motorola's proprietary trade secrets and confidential information from Motorola's protected computers for their individual benefit and the benefit of others, by and through nonsecure means into a nonsecure environment, thereby impairing the integrity and/or availability of such information.

Defendant Sheng's Unauthorized Activities with Defendants Lemko and Jin

96. Defendant Sheng is a citizen of China who has been studying or working in the U.S. as an engineer since 1999.

97. In 2006, Defendant Sheng worked as a software engineer for Defendant Lemko at its Schaumburg, Illinois offices.

98. In November 2006, Defendant Sheng began to work for Motorola as a software engineer. Nevertheless, Defendant Sheng secretly continued to work for and/or assist Defendant Lemko after she accepted employment with Motorola, as demonstrated by a January 29, 2007 e-mail in which Defendant Sheng stated, “[t]omorrow will be the last time that I help them. I actually felt the same way as you felt to Shaowei [Pan] and Lemko.”

99. In the course of her employment as a software engineer for Motorola, Defendant Sheng had access to Motorola’s proprietary trade secrets and confidential information in the performance of her duties.

100. Motorola reposed a high level of trust and confidence in Defendant Sheng’s trustworthiness, integrity, and fidelity to her obligations towards Motorola. These duties were memorialized in part through Defendant Sheng’s executed “Employee Confidentiality and Assignment of Inventions Agreement” and through her signed acknowledgment of Motorola’s “Code of Business Conduct.”

101. Motorola provided Defendant Sheng with a laptop computer for use in carrying out her assigned tasks. Defendant Sheng had access to Motorola’s secure internal computer networks through this laptop.

102. In the course of its investigation, Motorola discovered the presence of Lemko associated source code on Sheng’s Motorola-issued laptop, as well as evidence that the laptop had been connected by Sheng to a USB drive containing folders labeled “Lemko.”

103. While Defendant Sheng surreptitiously worked for and/or assisted Defendant Lemko while employed by Motorola, Defendant Sheng placed Lemko associated source code on the Motorola laptop issued to her, in violation of Motorola's policies.

104. Defendant Sheng also has communicated with Defendant Jin multiple times since Defendant Jin was detained at O'Hare International Airport by U.S. Customs on February 28, 2007, and, upon information and belief, such communications have been related to Lemko and unauthorized access to Motorola source code and other valuable Motorola proprietary trade secrets and confidential information.

105. On the evening of July 1, 2008, Motorola notified Defendant Sheng to report for a meeting with Motorola management the next day. Later that night and early in the morning of July 2, 2008, Defendant Sheng intentionally, knowingly, and with intent to defraud, accessed Motorola's protected laptop computer and, in furtherance of that fraud, downloaded a large number of files containing valuable Motorola proprietary trade secrets and confidential information from that protected laptop onto a non-Motorola, non-secure USB hard drive without authorization or exceeding her authorized access, and without Motorola's knowledge or consent, thereby impairing the integrity and/or availability of this information.

106. The next day, July 2, 2008, Motorola interviewed Defendant Sheng, and terminated her employment for violations of Motorola's policies.

107. To date, Motorola has incurred substantial losses, in excess of \$5,000 in a one-year period, due to Defendant Sheng's unauthorized access to Motorola's protected computers and unauthorized removal, possession, and impairment of Motorola's electronic files and documents, including without limitation, the costs of investigating Defendant Sheng's actions and assessing the damage she caused.

108. Defendant Sheng, individually and in concert with Defendant Lemko, Defendant Jin and others, without authorization or exceeding their authorized access, and without Motorola's knowledge or consent, intentionally, knowingly, and with intent to defraud accessed Motorola's protected computers and, in furtherance of that fraud, downloaded, uploaded, and transferred Motorola's proprietary trade secrets and confidential information for her own benefit and the benefit of others, including Defendants Lemko and Jin, by and through nonsecure means into a nonsecure environment, thereby impairing the integrity and/or availability of such information.

**Defendants Pan, Labun, Pyskir, Cai, Zhang, Favila, Saxena and Jin
Conspire to Form and Conduct A Fraudulent and Competing Business
While They Are Still Employed By Motorola**

109. Defendant Pan was hired by Motorola on about August 1, 1994 as a Staff Engineer for Motorola New Enterprises. Pan was employed full-time and paid a salary by Motorola through about April 2, 2004. In or before July 2002, without Motorola's knowledge or consent, Pan accepted employment with and/or began actively working on behalf of Defendant Lemko. Pan never disclosed this to Motorola, nor sought approval from Motorola for his simultaneous employment with Lemko.

110. Defendant Nicholas Labun was hired by Motorola on about September 25, 1989 as Director of Strategy, Motorola New Enterprises. Labun was employed full-time and paid a salary by Motorola through about May 10, 2004. In or before July 2002, without Motorola's knowledge or consent, Defendant Labun accepted employment with and/or began actively working on behalf of Defendant Lemko. Labun never disclosed this to Motorola, nor sought approval from Motorola for his simultaneous employment with Lemko.

111. Defendant Bohdan Pyskir was hired by Motorola on about January 7, 1993 as a Business Development Manager with Motorola Paging and Wireless Data Group. Pyskir was

employed full-time and paid a salary by Motorola through about March 31, 2004. In or before July 2002, without Motorola's knowledge or consent, Defendant Pyskir accepted employment with and/or began actively working on behalf of Defendant Lemko. Pyskir never disclosed this to Motorola, nor sought approval from Motorola for his simultaneous employment with Lemko.

112. Defendant Hechun Cai was hired by Motorola on about October 26, 1998 as "Lead Software Engineer reporting to ShaoWei Pan in the Cellular Infrastructure Group." Cai was employed full-time and paid a salary by Motorola through about May 19, 2005. In or before September 2002, without Motorola's knowledge or consent, Defendant Cai accepted employment with and/or began actively working on behalf of Defendant Lemko. Cai never disclosed this to Motorola, nor sought approval from Motorola for his simultaneous employment with Lemko.

113. Defendant Jinzhong Zhang was hired by Motorola on about May 19, 1995, and was employed full-time and paid a salary by Motorola from through about July 11, 2004. In or before September 2002, without Motorola's knowledge or consent, Defendant Zhang accepted employment with and/or began actively working on behalf of Defendant Lemko. Zhang never disclosed this to Motorola, nor sought approval from Motorola for his simultaneous employment with Lemko.

114. Defendant Angel Favila was hired by Motorola on about December 18, 1989 as a programmer with the Motorola Communications Sector. Favila is still employed full-time and paid a salary by Motorola. In or before June 2004 without Motorola's knowledge or consent, Defendant Favila accepted employment with and/or began actively working on behalf of Defendant Lemko. Favila never disclosed this to Motorola, nor sought approval from Motorola for his simultaneous employment with Lemko.

115. Defendant Ankur Saxena was employed full-time and paid a salary by Motorola from about May 31, 2000 through about August 2, 2005. In or before June 2004, without Motorola's knowledge or consent, Defendant Saxena accepted employment with and/or began actively working on behalf of Defendant Lemko. Saxena never disclosed his simultaneous employment with Lemko to Motorola, nor sought approval from Motorola for his simultaneous employment with Lemko..

116. Defendant Labun supervised Defendant Pan's and Defendant Pyskir's work at Motorola. Labun signed Pan's performance reviews as Pan's manager in 2000, 2001, 2002, and 2003. Labun signed Pyskir's performance reviews as Pyskir's manager in 2002 and 2003.

117. Defendant Pan supervised Defendant Cai's, Defendant Zhang's and Defendant Favila's work at Motorola. Pan signed Cai's performance reviews as Cai's manager each year between 1999 and 2004. Pan also signed Zhang's performance reviews as Zhang's manager each year between 1999 and 2004. Pan signed Favila's performance reviews as Favila's manager each year from 2001-2004.

118. Defendant Zhang supervised Defendant Saxena's and Defendant Jin's work at Motorola. Zhang signed Saxena's performance reviews as Saxena's manager in 2002, 2003 and 2004. Zhang signed Jin's performance reviews as Jin's manager in 2001, 2002 and 2003.

119. While they were employed by Motorola, Defendants Pan, Labun, Pyskir, Cai and Zhang, together with Defendant Howell, founded Defendant Lemko.

120. Defendants Pan, Labun, Pyskir and Howell began working on Lemko Corporation in or before 2002.

121. Defendants Vorick, Cai, Zhang and Desai began working for the benefit of Lemko in or before 2002.

122. By mid-2002, Defendants already had converted their efforts and work product as Motorola employees into a product for Lemko, and Defendants were arranging meetings with customers and competitors of Motorola to show them “a working demo of the Lemko system.”

123. Defendants Vorick, Pan, Labun, Pyskir, Zhang, Cai and Jin began discussing and working on Lemko patent submissions at least as early as September 2002, while Pan, Labun, Pyskir, Zhang and Jin were each employees of Motorola with a prior agreement to assign their inventions to Motorola.

123.1 Defendant Desai acting in concert with the other defendants, including Defendant Faye Vorick, engaged in various activities in 2002 and 2003 to obtain, under false pretenses, Motorola proprietary information relating to Motorola base stations and by assisting in efforts to acquire and induce Motorola employees to disclose proprietary information about the Motorola SC300 base station and other proprietary information relating to Motorola’s proprietary base transceiver station (BTS) technologies for the benefit of Lemko and others.

123.2 Defendant Desai acting by and through a company called Invium fraudulently induced Motorola to enter into a nondisclosure agreement (NDA) in January 2003 in order to acquire proprietary and secret information relating to Motorola’s proprietary BTS technologies which were misappropriated by Lemko and other defendants, including Defendants Pan and Pyskir, without Motorola’s knowledge, authorization and consent and in violation of the contractual obligations of the NDA.

123.3 In order to hide his secret relationship with Lemko and the secret activities of Defendants Pan, Pyskir and Labun, who were still employed by Motorola and working secretly for Lemko, Defendant Desai conspired with these Defendants to actively hide these

secret relationships during discussions with Motorola regarding the alleged business activities of Invium, which were in fact for the unauthorized benefit of Lemko and such other defendants.

123.4 Defendant Vorick actively assisted Defendant Desai in acquiring, disclosing and using Motorola proprietary information, including specifications for the Motorola SC300 product, and acquiring, disclosing and using Motorola proprietary information to draft business plans for Lemko via email communications from Defendant Pan's personal email account while Defendant Pan was still a full time employee of Motorola.

123.5 Defendant Vorick played a key role as the "front" person for Lemko's wrongful activities in exploiting Motorola's proprietary trade secrets and confidential information for the benefit of Lemko and others, when in fact many of the defendants involved in these wrongful activities were still employed as full time Motorola employees. At all times Defendant Vorick knew or had reason to know that Lemko was engaged in the wrongful acquisition, disclosure and use of Motorola proprietary information, without Motorola's authorization and consent.

123.6 Defendant Vorick actively participated in all the efforts to secretly obtain and exploit Motorola proprietary information for the benefit of Lemko and others; including researching the patent filing process for Lemko while Shaowei Pan was still employed at Motorola; contacting Motorola to obtain proprietary pricing and technical information; attempting to place an order for the Motorola Model SC300 base station; checking documents to make sure the "Motorola" proprietary legend was changed to the "Lemko" proprietary legend; preparing and revising Lemko presentations using misappropriated Motorola proprietary information and generally running various Lemko business operations as the Lemko VP of

Marketing and as a member of the Lemko management team during 2002 and 2003 while Defendants Pan, Pyskir and Labun were still full time employees of Motorola.

123.7 Defendant Desai also engaged in Lemko business development activities in 2002-2003 disguising the fact that Defendants Pan, Pyskir and Labun were still Motorola full time employees, and conspiring and assisting in secret activities to acquire, disclose and use Motorola proprietary trade secrets and confidential information that Defendant Desai knew or had reason to know were misappropriated from Motorola without Motorola's authorization and consent.

123.8 Both Defendants Desai and Vorick engaged in marketing and business activities to promote Lemko's alleged proprietary technologies, knowing that these secret proprietary technologies had been misappropriated from Motorola and that Defendants Labun, Pyskir and Pan were still working full time as Motorola employees and actively misappropriating Motorola trade secrets and proprietary information for the benefit of Lemko and others.

123.9 Defendant Vorick as a member of the secret Lemko management team (involving full time Motorola employees, Defendants Labun, Pan, Pyskir as well as Defendant Howell), actively engaged in efforts to obtain financing for Lemko's unauthorized business activities including the preparation of business plans and financial projections that would result from Lemko products derived from the misappropriation of Motorola proprietary information and trade secrets.

124. Defendants began conducting Lemko field trials at customer sites in or before 2003. These trials involved products built upon and containing Motorola's source code and other of Motorola's proprietary trade secrets and confidential information.

125. In January 2003, Lemko represented to investors that it was currently selling a product which required no further development time or expense.

126. Defendants Pan, Labun, Pyskir, Cai, Zhang, Favila, Saxena and Jin, individually and/or in concert, used Motorola assets and Motorola's proprietary research and development, source code, development tools and other trade secrets to develop and market a product, acquire investors, prepare and file patent applications, establish and run Lemko, and used Lemko to exploit and transfer Motorola proprietary information to entities in China and other parts of the world.

127. In 2002, 2003 and 2004, Defendants Pan, Labun, Pyskir, Cai and Zhang, individually and/or in concert, promoted Lemko's business at trade shows that they attended as Motorola employees, and/or made sales and technical presentations and conducted demonstrations and trials at potential customer sites around the world while they were working full-time for Motorola.

128. The products that Defendants attempted to sell and did sell on behalf of Lemko were developed by Motorola employees, at Motorola's time and expense, and with the use of Motorola's proprietary trade secrets and confidential information.

129. Defendants Pan, Labun, Pyskir, Cai, Zhang, Favila, Saxena and Jin, individually and/or in concert, hid their dual employment from potential Lemko investors and customers by failing to disclose their current employment status at Motorola, and/or by falsely representing that they were former employees of Motorola when in fact they were current employees of Motorola.

130. Defendants Pan, Labun, Pyskir, Cai, Zhang, Favila, Saxena and Jin, individually and/or in concert, further hid their dual employment from Motorola, by directing others to communicate with Motorola on their behalf and on Lemko's behalf.

131. Prior to March 17, 2003, Defendants Howell, Pan, Labun, and Pyskir formed IDC Holdings, LLC, an Illinois holding company in which they were each members, for the purpose of hiding the Motorola employees' direct involvement in Lemko. In January 2004, the Operating Agreement of IDC Holdings, LLC was amended to add Defendants Cai and Zhang as members. At that time, the six members of IDC Holdings, LLC collectively owned the majority of the stock of Lemko. IDC Holdings, LLC was voluntarily dissolved in September 2005.

132. Defendants Howell, Vorick and Desai knew or should have known that Defendants Pan, Labun, Pyskir, Cai, Zhang, Favila, Saxena and Jin were full-time Motorola employees who were improperly acquiring, disclosing and using Motorola trade secrets for the benefit of Defendant Lemko. Defendants Howell, Vorick and Desai were aware that these Defendants, who were employed at Motorola, improperly were engaging in activities on behalf of Defendant Lemko that presented a clear conflict of interest in regards to their employment at Motorola. Defendants Howell, Vorick and Desai actively aided in the cover up of these Defendants' full-time employment at Motorola and their improper conduct.

133. Pan acted as the Chief Technical Officer of Lemko from at least January 2003 until he resigned from Motorola and thereafter. As a Motorola employee, Pan had access to Motorola's computers and Motorola's proprietary trade secrets and confidential information.

134. Without Motorola's knowledge or consent, and exceeding his authorized access, on multiple occasions Defendant Pan obtained valuable proprietary and trade secret information

from Motorola's protected computers and forwarded the Motorola information to his personal email account.

135. Pan's non-Motorola computers contain Motorola source code and other of Motorola's proprietary trade secrets and confidential information, and many of these files were stored on Pan's computers for use at Lemko.

136. On multiple occasions, Pan transferred files containing Motorola's source code and other of Motorola's proprietary trade secrets and confidential information to Lemko, or through Lemko to third-parties for the benefit of Lemko.

137. On at least one occasion, the words "Copyright © 2001, Motorola, Inc." were removed from a Motorola source code file and the otherwise identical source code file was transferred to Lemko without the copyright notice and with an instruction that the attached files could be used to update Lemko code.

138. On October 12, 2006, more than two years after Defendant Pan had terminated his employment by Motorola, more than 300 files were copied to Pan's JAYPAN computer, all identical to the Motorola files recovered by the FBI from non-Motorola media during Defendant Jin's arrest. These files contain Motorola's proprietary trade secrets and confidential information, and nearly all of them were used in one or more Lemko customer trials.

139. An unusually large number of USB drives were plugged into Pan's and/or Wu's personal or Lemko computers, totaling at least 83 unique USB storage devices. At least one of these USB devices was attached to both Pan's computer and Defendant Jin's Motorola-issued laptop computer.

COUNT ONE

COMPUTER FRAUD AND ABUSE ACT

(Against Lemko, Pan, Jin, Wu, Bai, and Sheng)

140. Motorola repeats and realleges the averments of paragraphs 1-139 as if fully set forth herein.

141. All computers used by Defendants without authorization or in excess of authorized access, or to destroy or impair Motorola information, including but not limited to all servers, desktop computers, laptop computers, external hard drives, "Blackberry" and/or "Q" devices, and thumb drives, USB drives, and "flash" drives, were at all relevant times used in interstate commerce and are protected computers pursuant to the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(e). The Motorola proprietary trade secrets and confidential information is stored on, and may be accessed from, one or more of these protected computers owned by Motorola, access to which is strictly controlled via various security measures, including secret passwords, and all are used in or affect interstate or foreign communications or commerce.

142. Defendants intentionally accessed the secure, protected computers of Motorola or other protected computers without authorization or exceeding their authorization, and thereby obtained information from those protected computers, in violation of 18 U.S.C. § 1030(a)(2)(C).

143. Defendants knowingly and with the intent to defraud, accessed the secure, protected computers of Motorola or other protected computers, or caused others to access the secure, protected computers of Motorola, without authorization or in excess of their authorized access and in furtherance of the intended fraud obtained the valuable Motorola proprietary trade secrets and confidential information and/or other valuable information or the valuable use of the secure Motorola network and computers, which has a value exceeding five thousand dollars (\$5,000.00) in a one-year period, in violation of 18 U.S.C. § 1030(a)(4).

144. Defendants knowingly caused the transmission of a program, information, code, or command and/or intentionally accessed the protected computers of Motorola and/or other protected computers, and, as a result, intentionally and without authorization, recklessly caused damage and loss to the secure, protected computers of Motorola and/or other protected computers in violation of 18 U.S.C. § 1030(a)(5)(A)-(C).¹

145. Defendants, through their actions in violation of 18 U.S.C. § 1030(a)(2), (a)(4), and (a)(5)(A)-(C), have caused Motorola to incur losses for responding to and investigation of Defendants' misconduct, including damage and security assessments, exceeding five thousand dollars (\$5,000.00) during a one-year period in violation of 18 U.S.C. § 1030(g) and (c)(4)(A)(i)(I); the investigation of such losses continues.

146. In addition to an award of compensatory damages, Motorola also is entitled to injunctive relief pursuant to 18 U.S.C. § 1030(g), restraining and enjoining Defendants and all those in privity, concert or participation with Defendants from engaging in such wrongful acts in violation of 18 U.S.C. § 1030(a)(2), (a)(4), and (a)(5)(A)-(C).

WHEREFORE, Plaintiff respectfully requests that this Court enter the following relief against Defendants:

- a. enter judgment in favor of Motorola on Count One;
- b. award both preliminary and permanent injunctive relief pursuant to 18 U.S.C. § 1030, *et seq.*, restraining and enjoining Defendants and all those in privity, concert or participation with them from engaging in acts and practices in violation thereof;
- c. award compensatory damages pursuant to 18 U.S.C. § 1030, *et seq.*, in an amount in excess of \$5,000.00 to be proven at trial;

¹ By order of February 11, 2009, the Court dismissed Plaintiff's claim for violation of 18 U.S.C. § 1030(a)(5). Plaintiff recognizes the Court's ruling as current law of the case, but repleads its claim for violation of section 1030(a)(5) in this Second Amended Complaint in order to preserve the issue for appeal.

- d. enter an order compelling Defendants to return any and all of Plaintiff's proprietary trade secrets and confidential information including all types of scientific, technical and engineering information, files, documents, drawings, schematics, programs, object code, source code, designs, prototypes and the like, in Defendants' possession, custody or control, and wherever and however stored physically, electronically, graphically, photographically, or in writing, and all derivations and compilations and/or other memorializations of such purloined information; together with such other affirmative relief required to compel compliance with this order, including the use of electronic evidence experts and other technicians;
- e. enter an order compelling Defendants to disclose its actual and potential customers and any and all persons and entities to which Defendants disclosed Plaintiff's proprietary trade secrets and confidential information; and
- f. such further relief as this Court may deem just and proper, in law or equity.

COUNT TWO

**THREATENED OR ACTUAL
MISAPPROPRIATION OF TRADE SECRETS**

(Against All Defendants)

147. Motorola repeats and realleges the averments of paragraphs 1-139 as if fully set forth herein.

148. The Motorola proprietary trade secrets and confidential information, set forth individually and collectively in the preceding paragraphs of the Complaint, are statutory "trade secrets" protected by the Illinois Trade Secrets Act, 765 ILCS 1065/1 *et seq.*

149. At all times, Motorola has taken reasonable measures to protect the Motorola proprietary trade secrets and confidential information, and Motorola derives economic value and competitive advantage from such information not being generally known to the public or trade.

150. There exists the threatened or actual misappropriation of trade secrets by the Defendants, acting individually and in concert, to acquire, disclose and/or use, by improper

means, the Motorola proprietary trade secrets and confidential information for their own benefit and/or the benefit of others without or exceeding Motorola's authorization and consent.

151. Motorola has sustained and will continue to sustain damages, and Defendants have been and will continue to be unjustly enriched in an amount to be proven at trial, as a direct result of Defendants' threatened or actual misappropriation of the Motorola proprietary trade secrets and confidential information.

152. Defendants' threatened or actual misappropriation of the Motorola proprietary trade secrets and confidential information has been willful and malicious and entitles Motorola to exemplary damages and an award of attorneys' fees and costs pursuant to the Illinois Trade Secrets Act, 765 ILCS 1065/1 *et seq.*

153. Motorola also is entitled to injunctive relief to prevent the threatened or actual misappropriation of the Motorola proprietary trade secrets and confidential information by Defendants pursuant to the Illinois Trade Secrets Act, 765 ILCS 1065/1 *et seq.*

WHEREFORE, Plaintiff respectfully requests that this Court enter the following relief against Defendants:

- a. enter judgment in favor of Motorola on Count Two;
- b. both preliminary and permanent relief pursuant to 765 ILCS 1065/1, et seq. restraining and enjoining Defendant Lemko, its officers, directors, employees, agents, and all those in privity, concert or participation with it from the threatened or actual misappropriation of the Motorola proprietary trade secrets and confidential information;
- c. both preliminary and permanent relief pursuant to 765 ILCS 1065/1, et seq. restraining and enjoining Defendants Pan, Jin, Wu, Bai, Sheng, Labun, Pyskir, Cai, Zhang, Favila, Saxena, Howell, Vorick and Desai, and all those in privity, concert or participation with them from the threatened or actual misappropriation of the Motorola proprietary trade secrets and confidential information;
- d. a finding that Defendants' acts and conduct constitute the actual or threatened misappropriation of trade secrets in violation of 765 ILCS 1065/1, et seq., and that such acts and conduct are and have been willful and malicious;

- e. compensatory and increased damages sustained as a result of Defendants' wrongful actions, together with an accounting of Defendants' profits and unjust enrichment arising from such actions;
- f. an order compelling Defendants to return any and all of Plaintiff's proprietary trade secrets and confidential information including all types of scientific, technical and engineering information, files, documents, drawings, schematics, programs, object code, source code, designs, prototypes and the like, in Defendants' possession, custody or control, and wherever and however stored physically, electronically, graphically, photographically, or in writing, and all derivations and compilations and/or other memorializations of such purloined information; together with such other affirmative relief required to compel compliance with this order, including the use of electronic evidence experts and other technicians;
- g. an order compelling Defendants to disclose its actual and potential customers and any and all persons and entities to which Defendants disclosed Plaintiff's proprietary trade secrets and confidential information;
- h. attorneys' fees and costs pursuant to 765 ILCS 1065/1, et seq.; and
- i. such further relief as this Court may deem just and proper, in law or equity.

COUNT THREE

BREACH OF FIDUCIARY DUTY

(Against Defendants Jin, Wu, Bai, and Sheng)

154. Motorola repeats and realleges the averments of paragraphs 1-139 as if fully set forth herein.

155. Defendants Jin, Wu, Bai, and Sheng each held positions of trust and confidence with Motorola, and each owed Motorola a duty of loyalty as Motorola's employees.

156. Defendants Jin, Wu, Bai, and Sheng, individually and in concert, abused their respective positions of trust and confidence with Motorola to further their private interests, failed to protect the corporate property of Motorola, and deprived Motorola of profit or advantages in the marketplace.

157. Defendants Jin, Wu, Bai, and Sheng, by their actions individually and in concert, violated the duty of loyalty required of them as employees of Motorola not to engage in competition with Motorola while employed by Motorola.

158. Defendants Jin, Wu, Bai, and Sheng, individually and in concert, acted with fraud, oppression, and/or malice.

159. Motorola has sustained losses and damages as a direct and proximate result of Defendant's wrongful actions described herein in an amount to be determined at trial.

WHEREFORE, Plaintiff respectfully requests that this Court enter the following relief against Defendants:

- a. enter judgment in favor of Motorola on Count Three;
- b. compensatory damages, including disgorgement, for the breach of fiduciary duty by Defendants Jin, Wu, Bai, and Sheng;
- c. exemplary damages for the acts constituting breach of fiduciary duty committed with fraud, oppression, and/or malice; and
- d. such further relief as this Court may deem just and proper, in law or equity.

COUNT FOUR

BREACH OF FIDUCIARY DUTY

(against Defendants Pan, Labun, Pyskir, Cai, Zhang, Favila, and Saxena)

160. Motorola repeats and realleges the averments of paragraphs 1-139, as if fully set forth herein.

161. Defendants Pan, Pyskir, Cai, Zhang, Favila, and Saxena held positions of trust and confidence with Motorola, and each owed Motorola a duty of loyalty as Motorola's employees.

162. Defendant Labun was both an officer and employee of Motorola and therefore held a position of heightened trust and confidence with Motorola and owed Motorola a heightened duty of loyalty as an officer and employee of Motorola.

163. Defendants Labun, Pan, Pyskir, Cai, Zhang, Favila, and Saxena, individually and in concert, abused their respective positions of trust and confidence with Motorola to further their private interests, failed to protect the corporate property of Motorola, and deprived Motorola of profit or advantages in the marketplace.

164. Defendants Labun, Pan, Pyskir, Cai, Zhang, Favila, and Saxena, individually and in concert, violated the duty of loyalty required of them as employees of Motorola not to engage in competition with Motorola while employed by Motorola.

165. Defendants Labun, Pan, Pyskir, Cai, Zhang, Favila, and Saxena, individually and in concert, acted with fraud, oppression, and/or malice.

166. Motorola has sustained losses and damages as a direct and proximate result of Defendants' wrongful actions described herein.

WHEREFORE, Plaintiff respectfully requests that this Court enter the following relief against Defendants:

- a. enter judgment in favor of Motorola on Count Four;
- b. award compensatory damages in an amount to be determined at trial;
- c. order disgorgement of all payments, revenue, profits, monies, royalties and any other benefits derived or obtained by Defendants from the breach of their fiduciary duties to Motorola;
- d. award punitive damages for the acts constituting breach of fiduciary duty committed with fraud, oppression and/or malice in an amount sufficient to punish Defendants and deter such misconduct in the future;
- e. order restitution and forfeiture of all compensation and benefits paid to Defendants by Motorola during the period of the breach of Defendants' loyalty to Motorola; and
- f. such further relief as this Court may deem just and proper, in law or equity.

COUNT FIVE

USURPATION OF CORPORATE OPPORTUNITY

(Against Pan, Labun, Pyskir)

167. Motorola repeats and realleges the averments of paragraphs 1-139, as if fully set forth herein.

168. Defendant Pan, Defendant Labun and Defendant Pyskir held positions of authority and trust at Motorola, and were entrusted with Motorola's proprietary trade secrets and confidential information.

169. Defendants owed certain fiduciary duties to Motorola on account of their positions at Motorola.

170. Defendants used Motorola's proprietary trade secrets and confidential information for their own benefit and for the benefit of Defendant Lemko, both before and after the termination of their employment by Motorola.

171. Defendants failed to disclose business opportunities to Motorola and, instead, diverted opportunities that were developed through the use of Motorola assets to Defendant Lemko.

172. Defendants' conduct violated their duty of loyalty to their employer, Motorola, and their obligation to act in the best interest of Motorola.

173. Defendants' breaches of their fiduciary duty were a proximate cause of injury to Motorola.

WHEREFORE, Plaintiff respectfully requests that this Court enter the following relief against Defendants:

- a. enter judgment in favor of Motorola on Count Five;
- b. award compensatory damages in an amount to be determined at trial;

- c. order disgorgement of all payments, revenue, profits, monies, royalties and any other benefits derived or obtained by Defendants from the breach of their fiduciary duties to Motorola;
- d. award punitive damages for the acts constituting breach of fiduciary duty committed with fraud, oppression and/or malice in an amount sufficient to punish Defendants and deter such misconduct in the future;
- e. order restitution and forfeiture of all compensation and benefits paid to Defendants Pan, Labun and Pyskir by Motorola during the period of the breach of Defendants' loyalty to Motorola; and
- f. such further relief as this Court may deem just and proper, in law or equity.

COUNT SIX

DECLARATORY JUDGMENT OF PATENT OWNERSHIP

(Against Lemko, Pan And Labun)

174. Motorola repeats and realleges the averments of paragraphs 1-139, 188-220 as if fully set forth herein.

175. Defendant Pan's employment responsibilities at Motorola included assisting in the development of innovative mobile communication system technologies, including the conception and design of distributed mobile communications systems, methods and devices.

176. Defendant Labun's employment responsibilities at Motorola included the development of new business, through the creation and commercialization of proprietary Motorola technology, and assisting in the development and commercialization of innovative mobile communication system technologies, including the conception and design of distributed mobile communications systems, methods and devices.

177. Beginning in or before September 2002, Defendants Pan and Labun began planning patent filings on behalf of Lemko for inventions, innovations or ideas that they developed or conceived during their employment at Motorola, and which related to the actual or

anticipated business activities of Motorola, and/or which resulted from or were suggested by work which Pan and Labun did for Motorola.

178. Pan and Labun used Motorola's offices, equipment, laboratories, other facilities, supplies, materials, and/or subordinates' time to substantially complete the inventions developed and conceived during their employment at Motorola.

179. Pan and Labun failed to disclose their inventions, innovations and ideas to Motorola, and further failed to submit records of these inventions to Motorola, as required by their agreements with Motorola and their fiduciary duties to Motorola.

180. Lemko is the assignee of certain patents and patent applications disclosing and claiming a system, method and device for providing communications using a distributed mobile architecture, namely U.S. Patent No. 7,539,158, U.S. Patent No. 7,486,967, U.S. Patent No. 7,548,763, and U.S. Patent No. 7,653,414 (hereinafter the "Lemko Patents"); U.S. Patent Application Nos. 11/393,993, 11/451,238, 11/858,762, 11/955,017, 12/108,209, 12/146,618, 12/163,601, 12/171,840, 12/172,639, 12/238,269, 12/425,147 and 12/471,253 and International Patent Application Nos. PCT/US2009/045951 and PCT/US2009/045957 (hereinafter the "Lemko Patent Applications").

181. The named inventor(s) listed on the Lemko Patents and the Lemko Patent Applications are Pan and/or Pan and Labun.

182. The patent application leading to U.S. Patent 7,539,158 was filed on November 8, 2004, only months after Pan and Labun departed from Motorola.

183. The patent applications leading to U.S. Patent 7,486,967 and U.S. Patent No. 7,548,763, respectively, were each filed on April 13, 2005.

184. Each of the inventions disclosed and claimed in the Lemko Patents and the Lemko Patent Applications were developed and/or conceived by Pan, or by Pan and Labun, or by Pan and/or Labun jointly with others at Motorola, during the term of their employment at Motorola.

185. There is an actual and justiciable controversy regarding the rightful owner of the invention or inventions disclosed and claimed in the Lemko Patents and the Lemko Patent Applications, and all inventions derived therefrom.

186. Motorola is entitled to a declaration that the inventions disclosed and claimed in the Lemko Patents and the Lemko Patent Applications, and all inventions derived therefrom, were previously assigned to Motorola by inventors Pan and Labun.

187. Motorola thus seeks a declaration from this Court pursuant to the Declaratory Judgment Act, 28 U.S.C. §§ 2201, that Motorola is the rightful owner of the Lemko Patents and the Lemko Patent Applications and all other inventions and patent applications pending worldwide that were derived from the inventions claimed in the Lemko Patents and the Lemko Patent Applications, and any other inventions developed by Defendants at Motorola and using Motorola resources.

WHEREFORE, Plaintiff, Motorola, Inc., respectfully requests that this Court enter the following relief against Defendants Lemko, Pan and Labun:

- a. a declaration that Motorola owns all right, title and interest to the invention or inventions disclosed and claimed in the Lemko Patents, and all inventions derived therefrom;
- b. a declaration that Motorola owns all right, title and interest to the invention or inventions disclosed and claimed in the Lemko Patent Applications, all inventions derived therefrom, and any patent, continuation patent, or divisional patent that may issue therefrom;
- c. order Pan and Labun to make a full and complete disclosure to Motorola of the invention or inventions disclosed in the Lemko Patent Applications;

- d. order Lemko, Pan and Labun to assign to Motorola all of their right, title and interest in the Lemko Patents, and any continuation or divisional patents that may issue therefrom.
- e. order Lemko, Pan and Labun to assign to Motorola all of their right, title and interest in the Lemko Patent Applications, and any patents issuing from such applications and all worldwide right, title and interest to the invention disclosed therein;
- f. enter a preliminary and permanent injunction enjoining Lemko, Pan and Labun, and those persons in active concert with them, from employing the methods, or from making, using, offering to sell or selling, or importing into the United States, the apparatus claimed in the Lemko Patents;
- g. enter a preliminary and permanent injunction enjoining Lemko, Pan and Labun, and those persons in active concert with them, from employing the methods or from making, using, offering to sell or selling, or importing into the United States the apparatus claimed in the Lemko Patent Applications as of the issue date of any patent which issues from such applications; and
- h. grant such other and further relief as this Court deems appropriate under the circumstances.

COUNT SEVEN

BREACH OF CONTRACT

(Against Pan)

188. Motorola repeats and realleges the averments of paragraphs 1-139, 175-187, as if fully set forth herein.

189. In consideration of his employment at Motorola and the salary and wages paid to him by Motorola, on August 1, 1994, Pan voluntarily executed an Employment Agreement with Motorola in the same form and substance as the attached **EXHIBIT A**.

190. In the Employment Agreement, Pan agreed not to use, publish, or otherwise disclose to others, either during or subsequent to his employment by Motorola, any confidential information of Motorola, or Motorola's customers and suppliers.

191. In the Employment Agreement, Pan further agreed that upon termination of his employment by Motorola he would promptly deliver to Motorola all documents and other records belonging to Motorola or relating to the business activities of Motorola.

192. In the Employment Agreement, Pan assigned to Motorola the entire right, title and interest to any inventions, innovations or ideas developed or conceived by Pan during his employment at Motorola, as follows:

I hereby assign to Motorola as its exclusive property the entire right, title and interest in all my inventions, innovations, or ideas developed or conceived by me solely, or jointly with others, at any time during the term of my employment and which inventions, innovations, or ideas relate to the actual or anticipated business activities of Motorola, or result from, or are suggested by, work which I do for Motorola.

193. In the Employment Agreement, Pan further agreed to make and maintain written records of his inventions, innovations or ideas, and to submit such records and any supplemental oral disclosures to designated representatives of Motorola, and to provide Motorola assistance in obtaining patents and other legal protection for inventions or innovations in the United States and any other country.

194. Defendant Pan further signed a Software Licensing, Information Protection and Non-Disclosure Agreement on or about August 1, 1994, whereby he agreed to use Motorola's computer resources and systems only for management-approved business purposes.

195. In the Software Licensing, Information Protection and Non-Disclosure Agreement, Pan further agreed not to copy, disclose or use any confidential or proprietary information which is owned by or entrusted to Motorola except to perform his job responsibilities.

196. On or about August 1, 1994, Pan acknowledged that he had been provided with a copy of the Motorola "Code of Conduct" and understood that he was required to abide by its provisions, including that Pan "may not work for or receive payments for services from any competitor, customer, distributor or supplier of Motorola without prior approval," and further that Pan was required to "disclose any situation that may be or appear to be a conflict of interest."

197. On or about March 31, 2004, Pan signed an Employee Separation Statement. Pursuant to this Statement Pan reconfirmed that he would not use or publish or otherwise disclose to others any confidential information of Motorola or its customers, and acknowledged that such confidential information existed not only within the scope of his immediate work at Motorola, but also in other work areas at Motorola to which he was exposed. Further, Pan represented that he had delivered to Motorola all documents and other records relating to the business activities of Motorola and other items belonging to Motorola, and agreed to return any Motorola items remaining in his possession within three (3) days. Further, Pan represented that he had complied with the terms of the Employment Agreement regarding the submission of inventions to Motorola.

198. Pan has breached his agreements with Motorola by copying, using and/or disclosing Motorola confidential and proprietary information for purposes other than in the performance of his job duties for Motorola, and by retaining, using and disclosing Motorola confidential and proprietary information to Lemko and other third parties, and by working for Lemko during the term of his employment by Motorola without disclosing the conflict of interest to Motorola or obtaining the prior approval of Motorola.

199. Pan has further breached his agreements with Motorola by failing to assign to Motorola the rights, title and interest in the inventions disclosed and claimed in the Lemko Patents and the Lemko Patent Applications, and instead assigning the Lemko Patents and the Lemko Patent Applications to Defendant Lemko.

200. Motorola has been injured by Pan's breaches of the foregoing agreements.

201. Pan's failure to disclose to Motorola the inventions, innovations or ideas that he developed or conceived while working for Motorola has caused, and will continue to cause, irreparable harm to Motorola, for which there is no adequate remedy at law.

202. Pan's failure to submit records of his inventions to Motorola or to provide Motorola assistance in obtaining patents and other legal protection has caused, and will continue to cause, irreparable harm to Motorola, for which there is no adequate remedy at law.

203. Pan's failure to assign the inventions to Motorola has caused, and will continue to cause, irreparable harm to Motorola, for which there is no adequate remedy at law.

WHEREFORE, Plaintiff, Motorola, Inc., respectfully requests that this Court enter the following relief against Defendant Pan:

- a. enter judgment in favor of Motorola on Count Seven;
- b. award compensatory damages in an amount to be determined at trial;
- c. order restitution and forfeiture of all compensation and benefits paid to Defendant Pan by Motorola during the period of the breach of Defendant Pan's loyalty to Motorola;
- d. order specific performance by Pan to comply with and satisfy his contractual obligations to Motorola;
- e. imposition of a constructive trust in favor of Motorola over all revenues or other benefits derived from the Lemko Patents or Patent Applications; and
- f. such further relief as this Court may deem just and proper, in law or equity.

COUNT EIGHT

BREACH OF CONTRACT

(Against Labun)

204. Motorola repeats and realleges the averments of paragraphs 1-139, 175-187, as if fully set forth herein.

205. In consideration of his employment at Motorola and the salary and wages paid to him by Motorola, on September 15, 1989, Labun voluntarily executed an Employment Agreement with Motorola in the same form and substance as the attached **EXHIBIT A**.

206. In the Employment Agreement, Labun agreed not to use, publish, or to otherwise disclose to others, either during or subsequent to his employment by Motorola, any confidential information of Motorola, or Motorola's customers and suppliers.

207. In his Employment Agreement, Labun further agreed that upon termination of his employment by Motorola he would promptly deliver to Motorola all documents and other records belonging to Motorola or relating to the business activities of Motorola.

208. In the Employment Agreement, Labun assigned to Motorola the entire right, title and interest to any inventions, innovations or ideas developed or conceived by Labun during his employment at Motorola, as follows:

I hereby assign to Motorola as its exclusive property the entire right, title and interest in all my inventions, innovations, or ideas developed or conceived by me solely, or jointly with others, at any time during the term of my employment and which inventions, innovations, or ideas relate to the actual or anticipated business activities of Motorola, or result from, or are suggested by, work which I do for Motorola.

209. In the Employment Agreement, Labun further agreed to make and maintain written records of his inventions, innovations or ideas, and to submit such records and any

supplemental oral disclosures to designated representatives of Motorola, and to provide Motorola assistance in obtaining patents and other legal protection for inventions or innovations in the United States and any other country.

210. On or about September 15, 1989, Labun acknowledged that he had been provided with a copy of the Motorola “Code of Conduct” and understood that he was required to abide by its provisions, including that Labun “may not work for or receive payments for services from any competitor, customer, distributor or supplier of Motorola without prior approval,” and further that Labun was required to “disclose any situation that may be or appear to be a conflict of interest.”

211. Defendant Labun further signed a Software Licensing, Information Protection and Non-Disclosure Agreement, whereby he agreed to use Motorola’s computer resources and systems only for management-approved business purposes.

212. In the Software Licensing, Information Protection and Non-Disclosure Agreement, Labun further agreed not to copy, disclose or use any confidential or proprietary information which is owned by or entrusted to Motorola except to perform his job responsibilities.

213. On or about May 11, 2004, Labun entered into a Separation and Release Agreement with Motorola. Pursuant to this Separation and Release Agreement, Motorola agreed to pay to Labun a lump sum separation payment and other benefits. Labun agreed to maintain the confidentiality of Motorola’s confidential or proprietary information and trade secrets in accordance with agreements previously signed by Labun and with the law applicable to Labun as an officer of Motorola, including but not limited to state trade secret protection statutes and Labun’s common law fiduciary duty and duty of loyalty. Labun further agreed (a) that he would

give Motorola advance written notice of his intent to disclose any potentially confidential information obtained by Labun as a result of his employment by Motorola; (b) that he would not perform any duties or responsibilities for any third party that would involve the disclosure of Motorola confidential and/or proprietary information or trade secrets or that would present a reasonable possibility of such disclosure, (c) that he would not recruit, solicit or induce, or cause, allow, permit or aid others to recruit, solicit or induce, or to communicate in support of those activities, any employee of Motorola to terminate his/her employment with Motorola and/or to seek employment with Labun's new or prospective employer, or any other company, and (d) that he would immediately inform Motorola about any new employment, start up business or self-employment in which he engaged in the two-year period following his May 10, 2004 separation date. Labun further agreed to repay to Motorola the sums that he received pursuant to the Separation Agreement and other benefits upon Labun's breach of the Separation Agreement.

214. Labun has breached the foregoing agreements with Motorola by copying, using and/or disclosing Motorola confidential and proprietary information for purposes other than in the performance of his job duties for Motorola, and by retaining, using and disclosing Motorola confidential and proprietary information to Lemko and other third parties, and by working for Lemko during the term of his employment by Motorola without obtaining the prior approval of Motorola or disclosing the conflict of interest to Motorola.

215. Labun has further breached the foregoing agreements with Motorola by failing to assign to Motorola the rights, title and interest in the inventions disclosed and claimed in the Lemko Patents and the Lemko Patent Applications, and instead assigning the Lemko Patents and the Lemko Patent Applications to Defendant Lemko.

216. Labun has further breached the foregoing agreements with Motorola by recruiting, soliciting or inducing employees of Motorola to terminate their employment with Motorola and to seek employment with Lemko.

217. Motorola has been injured by Labun's breaches of the foregoing agreements.

218. Labun's failure to disclose to Motorola the inventions, innovations or ideas that he developed or conceived while working for Motorola has caused, and will continue to cause, irreparable harm to Motorola, for which there is no adequate remedy at law.

219. Labun's failure to submit records of his inventions to Motorola or to provide Motorola assistance in obtaining patents and other legal protection has caused, and will continue to cause, irreparable harm to Motorola, for which there is no adequate remedy at law.

220. Labun's failure to assign the inventions to Motorola has caused, and will continue to cause, irreparable harm to Motorola, for which there is no adequate remedy at law.

WHEREFORE, Plaintiff, Motorola, Inc., respectfully requests that this Court enter the following relief against Defendant Labun:

- a. enter judgment in favor of Motorola on Count Eight;
- b. award compensatory damages in an amount to be determined at trial
- c. order restitution and forfeiture of all compensation and benefits paid to Defendant Labun by Motorola during the period of the breach of Defendant Labun's loyalty to Motorola;
- d. order specific performance by Labun to comply with and satisfy his contractual obligations to Motorola;
- e. imposition of a constructive trust in favor of Motorola over all revenues or other benefits derived from the Lemko Patents or Patent Applications; and
- f. such further relief as this Court may deem just and proper, in law or equity.

COUNT NINE

BREACH OF CONTRACT

(Against Pyskir)

221. Motorola repeats and realleges the averments of paragraphs 1-139, as if fully set forth herein.

222. In consideration of his employment at Motorola and the salary and wages paid to him by Motorola, on July 6, 1993, Pyskir voluntarily executed an Employment Agreement with Motorola in the same form and substance as the attached **EXHIBIT A**.

223. In the Employment Agreement, Pyskir agreed not to use, publish, or otherwise disclose to others, either during or subsequent to his employment by Motorola, any confidential information of Motorola, or Motorola's customers and suppliers.

224. In his Employment Agreement, Pyskir further agreed that upon termination of his employment by Motorola he would promptly deliver to Motorola all documents and other records belonging to Motorola or relating to the business activities of Motorola.

225. In the Employment Agreement, Pyskir assigned to Motorola the entire right, title and interest to any inventions, innovations or ideas developed or conceived by Pyskir during his employment at Motorola, as follows:

I hereby assign to Motorola as its exclusive property the entire right, title and interest in all my inventions, innovations, or ideas developed or conceived by me solely, or jointly with others, at any time during the term of my employment and which inventions, innovations, or ideas relate to the actual or anticipated business activities of Motorola, or result from, or are suggested by, work which I do for Motorola.

226. In the Employment Agreement, Pyskir further agreed to make and maintain written records of his inventions, innovations or ideas, and to submit such records and any

supplemental oral disclosures to designated representatives of Motorola, and to provide Motorola assistance in obtaining patents and other legal protection for inventions or innovations in the United States and any other country.

227. On or about July 6, 1993, Pyskir acknowledged that he had been provided with a copy of the Motorola "Code of Conduct" and understood that he was required to abide by its provisions, including that Pyskir "may not work for or receive payments for services from any competitor, customer, distributor or supplier of Motorola without prior approval," and further that Pyskir was required to "disclose any situation that may be or appear to be a conflict of interest."

228. On or about March 25, 2004, Pyskir signed an Employment Termination Statement. Pursuant to this Statement Pyskir reconfirmed that he would not use or publish or otherwise disclose to others any confidential information of Motorola or its customers, and acknowledged that such confidential information existed not only within the scope of his immediate work at Motorola, but also in other work areas at Motorola to which he was exposed. Further, Pyskir represented that he had delivered to Motorola all documents and other records relating to the business activities of Motorola and other items belonging to Motorola, and agreed to return any Motorola items remaining in his possession within three (3) days. Further, Pyskir represented that he had complied with the terms of the Employment Agreement regarding the submission of inventions to Motorola.

229. Pyskir has breached his agreements with Motorola by copying, using and/or disclosing Motorola confidential and proprietary information for purposes other than in the performance of his job duties for Motorola, and by retaining, using and disclosing Motorola confidential and proprietary information to Lemko and other third parties, and by working for

Lemko during the term of his employment by Motorola without obtaining the prior approval of Motorola or disclosing the conflict of interest to Motorola.

230. Motorola has been injured by Pyskir's breaches of the foregoing agreements.

WHEREFORE, Plaintiff, Motorola, Inc., respectfully requests that this Court enter the following relief against Defendant Pyskir:

- a. enter judgment in favor of Motorola on Count Nine;
- b. award compensatory damages in an amount to be determined at trial
- c. order restitution and forfeiture of all compensation and benefits paid to Defendant Pyskir by Motorola during the period of the breach of Defendant Pyskir's loyalty to Motorola; and
- d. such further relief as this Court may deem just and proper, in law or equity.

COUNT TEN

BREACH OF CONTRACT

(Against Cai)

231. Motorola repeats and realleges the averments of paragraphs 1-139, as if fully set forth herein.

232. In consideration of his employment at Motorola and the salary and wages paid to him by Motorola, October 26, 1998, Cai voluntarily executed an Employment Agreement with Motorola in the same form and substance as the attached **EXHIBIT A**.

233. In the Employment Agreement, Cai agreed not to use, publish, or otherwise disclose to others, either during or subsequent to his employment by Motorola, any confidential information of Motorola, or Motorola's customers and suppliers.

234. In his Employment Agreement, Cai further agreed that upon termination of his employment by Motorola he would promptly deliver to Motorola all documents and other records belonging to Motorola or relating to the business activities of Motorola.

235. In the Employment Agreement, Cai assigned to Motorola the entire right, title and interest to any inventions, innovations or ideas developed or conceived by Cai during his employment at Motorola, as follows:

I hereby assign to Motorola as its exclusive property the entire right, title and interest in all my inventions, innovations, or ideas developed or conceived by me solely, or jointly with others, at any time during the term of my employment and which inventions, innovations, or ideas relate to the actual or anticipated business activities of Motorola, or result from, or are suggested by, work which I do for Motorola.

236. Cai further agreed to make and maintain written records of his inventions, innovations or ideas, and to submit such records and any supplemental oral disclosures to designated representatives of Motorola, and to provide Motorola assistance in obtaining patents and other legal protection for inventions or innovations in the United States and any other country.

237. Defendant Cai further signed a Software Licensing, Information Protection and Non-Disclosure Agreement on or about October 26, 1998, whereby he agreed to use Motorola's computer resources and systems only for management-approved business purposes.

238. In the Software Licensing, Information Protection and Non-Disclosure Agreement, Cai further agreed not to copy, disclose or use any confidential or proprietary information which is owned by or entrusted to Motorola except to perform his job responsibilities.

239. On or about October 26, 1998, Cai signed an Acknowledgement that he had been provided with a copy of the Motorola "Code of Conduct" and understood that he was required to abide by its provisions as an ongoing condition of his employment at Motorola and understood that he was required to abide by its provisions, including that Cai "may not work for or receive

payments for services from any competitor, customer, distributor or supplier of Motorola without prior approval,” and further that Cai was required to “disclose any situation that may be or appear to be a conflict of interest.”

240. Cai has breached his agreements with Motorola by copying, using and/or disclosing Motorola confidential and proprietary information for purposes other than in the performance of his job duties for Motorola, and by retaining, using and disclosing Motorola confidential and proprietary information to Lemko and other third parties, and by working for Lemko during the term of his employment by Motorola without obtaining the prior approval of Motorola or disclosing the conflict of interest to Motorola.

241. Motorola has been injured by Cai’s breaches of the foregoing agreements.

WHEREFORE, Plaintiff, Motorola, Inc., respectfully requests that this Court enter the following relief against Defendant Cai:

- a. enter judgment in favor of Motorola on Count Ten;
- b. award compensatory damages in an amount to be determined at trial
- c. order restitution and forfeiture of all compensation and benefits paid to Defendant Cai by Motorola during the period of the breach of Defendant Cai’s loyalty to Motorola; and
- d. such further relief as this Court may deem just and proper, in law or equity.

COUNT ELEVEN

BREACH OF CONTRACT

(Against Zhang)

242. Motorola repeats and realleges the averments of paragraphs 1-139, as if fully set forth herein.

243. In consideration of his employment at Motorola and the salary and wages paid to him by Motorola, on May 19, 1995, Zhang voluntarily executed an Employment Agreement with Motorola in the same form and substance as the attached **EXHIBIT A**.

244. In the Employment Agreement, Zhang agreed not to use, publish, or otherwise disclose to others, either during or subsequent to his employment by Motorola, any confidential information of Motorola, or Motorola's customers and suppliers.

245. In his Employment Agreement, Zhang further agreed that upon termination of his employment by Motorola he would promptly deliver to Motorola all documents and other records belonging to Motorola or relating to the business activities of Motorola.

246. In the Employment Agreement, Zhang assigned to Motorola the entire right, title and interest to any inventions, innovations or ideas developed or conceived by Zhang during his employment at Motorola, as follows:

I hereby assign to Motorola as its exclusive property the entire right, title and interest in all my inventions, innovations, or ideas developed or conceived by me solely, or jointly with others, at any time during the term of my employment and which inventions, innovations, or ideas relate to the actual or anticipated business activities of Motorola, or result from, or are suggested by, work which I do for Motorola.

247. In the Employment Agreement, Zhang further agreed to make and maintain written records of his inventions, innovations or ideas, and to submit such records and any supplemental oral disclosures to designated representatives of Motorola, and to provide Motorola assistance in obtaining patents and other legal protection for inventions or innovations in the United States and any other country.

248. In further consideration of his employment at Motorola, Defendant Zhang signed a Software Licensing, Information Protection and Non-Disclosure Agreement, whereby he

agreed to use Motorola's computer resources and systems only for management-approved business purposes.

249. In the Software Licensing, Information Protection and Non-Disclosure Agreement, Zhang further agreed not to copy, disclose or use any confidential or proprietary information which is owned by or entrusted to Motorola except to perform his job responsibilities.

250. In further consideration of his employment at Motorola, Zhang acknowledged that he had been provided with a copy of the Motorola "Code of Conduct" and understood that he was required to abide by its provisions, including that Zhang "may not work for or receive payments for services from any competitor, customer, distributor or supplier of Motorola without prior approval," and further that Zhang was required to "disclose any situation that may be or appear to be a conflict of interest."

251. On or about January 21, 2005, Zhang signed an Employee Separation Statement. Pursuant to this Statement Zhang reconfirmed that he would not use or publish or otherwise disclose to others any confidential information of Motorola or its customers, and acknowledged that such confidential information existed not only within the scope of his immediate work at Motorola, but also in other work area at Motorola to which he was exposed. Further, Zhang represented that he had delivered to Motorola all documents and other records relating to the business activities of Motorola and other items belonging to Motorola, and agreed to return any Motorola items remaining in his possession within three (3) days. Further, Zhang represented that he had complied with the terms of the Employment Agreement regarding the submission of inventions to Motorola.

252. Zhang has breached his agreements with Motorola by copying, using and/or disclosing Motorola confidential and proprietary information for purposes other than in the performance of his job duties for Motorola, and by retaining, using and disclosing Motorola confidential and proprietary information to Lemko and other third parties, and by working for Lemko during the term of his employment by Motorola without obtaining the prior approval of Motorola or disclosing the conflict of interest to Motorola.

253. Motorola has been injured by Zhang's breaches of the foregoing agreements.

WHEREFORE, Plaintiff, Motorola, Inc., respectfully requests that this Court enter the following relief against Defendant Zhang:

- a. enter judgment in favor of Motorola on Count Eleven;
- b. award compensatory damages in an amount to be determined at trial
- c. order restitution and forfeiture of all compensation and benefits paid to Defendant Zhang by Motorola during the period of the breach of Defendant Zhang's loyalty to Motorola; and
- d. such further relief as this Court may deem just and proper, in law or equity.

COUNT TWELVE

BREACH OF CONTRACT

(Against Favila)

254. Motorola repeats and realleges the averments of paragraphs 1-139, as if fully set forth herein.

255. In consideration of his employment at Motorola and the salary and wages paid to him by Motorola, on December 18, 1989, Favila voluntarily executed an Employment Agreement with Motorola in the same form and substance as the attached **EXHIBIT A**.

256. In the Employment Agreement, Favila agreed not to use, publish, or otherwise disclose to others, either during or subsequent to his employment by Motorola, any confidential information of Motorola, or Motorola's customers and suppliers.

257. In his Employment Agreement, Favila further agreed that upon termination of his employment by Motorola he would promptly deliver to Motorola all documents and other records belonging to Motorola or relating to the business activities of Motorola.

258. In the Employment Agreement, Favila assigned to Motorola the entire right, title and interest to any inventions, innovations or ideas developed or conceived by Favila during his employment at Motorola, as follows:

I hereby assign to Motorola as its exclusive property the entire right, title and interest in all my inventions, innovations, or ideas developed or conceived by me solely, or jointly with others, at any time during the term of my employment and which inventions, innovations, or ideas relate to the actual or anticipated business activities of Motorola, or result from, or are suggested by, work which I do for Motorola.

259. In the Employment Agreement, Favila further agreed to make and maintain written records of his inventions, innovations or ideas, and to submit such records and any supplemental oral disclosures to designated representatives of Motorola, and to provide Motorola assistance in obtaining patents and other legal protection for inventions or innovations in the United States and any other country.

260. Defendant Favila further signed a Software Licensing, Information Protection and Non-Disclosure Agreement on or about June 22, 1994, whereby he agreed to use Motorola's computer resources and systems only for management-approved business purposes.

261. In the Software Licensing, Information Protection and Non-Disclosure Agreement, Favila further agreed not to copy, disclose or use any confidential or proprietary

information which is owned by or entrusted to Motorola except to perform his job responsibilities.

262. On or about December 18, 1989, Favila acknowledged that he had been provided with a copy of the Motorola "Code of Conduct" and understood that he was required to abide by its provisions, including that Favila "may not work for or receive payments for services from any competitor, customer, distributor or supplier of Motorola without prior approval," and further that Favila was required to "disclose any situation that may be or appear to be a conflict of interest."

263. Favila has breached the foregoing agreements with Motorola by copying, using and/or disclosing Motorola confidential and proprietary information for purposes other than in the performance of his job duties for Motorola, and by retaining, using and disclosing Motorola confidential and proprietary information to Lemko and other third parties, and by working for Lemko during the term of his employment by Motorola without obtaining the prior approval of Motorola or disclosing the conflict of interest to Motorola.

264. Motorola has been injured by Favila's breaches of the foregoing agreements.

WHEREFORE, Plaintiff, Motorola, Inc., respectfully requests that this Court enter the following relief against Defendant Favila:

- a. enter judgment in favor of Motorola on Count Twelve;
- b. award compensatory damages in an amount to be determined at trial
- c. order restitution and forfeiture of all compensation and benefits paid to Defendant Favila by Motorola during the period of the breach of Defendant Favila's loyalty to Motorola; and
- d. such further relief as this Court may deem just and proper, in law or equity.

COUNT THIRTEEN

BREACH OF CONTRACT

(Against Saxena)

265. Motorola repeats and realleges the averments of paragraphs 1-139, as if fully set forth herein.

266. In consideration of his employment at Motorola and the salary and wages paid to him by Motorola, on May 30, 2000 and July 23, 2001, Saxena voluntarily executed Employment Agreements with Motorola in the same form and substance as the attached **EXHIBIT A**.

267. In the Employment Agreements, Saxena agreed not to use, publish, or otherwise disclose to others, either during or subsequent to his employment by Motorola, any confidential information of Motorola, or Motorola's customers and suppliers.

268. In his Employment Agreements, Saxena further agreed that upon termination of his employment by Motorola he would promptly deliver to Motorola all documents and other records belonging to Motorola or relating to the business activities of Motorola.

269. In the Employment Agreements, Saxena assigned to Motorola the entire right, title and interest to any inventions, innovations or ideas developed or conceived by Saxena during his employment at Motorola, as follows:

I hereby assign to Motorola as its exclusive property the entire right, title and interest in all my inventions, innovations, or ideas developed or conceived by me solely, or jointly with others, at any time during the term of my employment and which inventions, innovations, or ideas relate to the actual or anticipated business activities of Motorola, or result from, or are suggested by, work which I do for Motorola.

270. In the Employment Agreements, Saxena further agreed to make and maintain written records of his inventions, innovations or ideas, and to submit such records and any

supplemental oral disclosures to designated representatives of Motorola, and to provide Motorola assistance in obtaining patents and other legal protection for inventions or innovations in the United States and any other country.

271. On or about May 30, 2000 and July 23, 2001, Saxena acknowledged that he had been provided with a copy of the Motorola "Code of Conduct" and understood that he was required to abide by its provisions, including that Saxena "may not work for or receive payments for services from any competitor, customer, distributor or supplier of Motorola without prior approval," and further that Saxena was required to "disclose any situation that may be or appear to be a conflict of interest."

272. On or about August 2, 2005, Saxena signed an Acknowledgment of Continuing Obligations Under Any Agreements Related to Confidential Information. Pursuant to this Acknowledgment Saxena reconfirmed that he would maintain Motorola's Confidential Information and Intellectual Property including all information and trade secrets (whether or not specifically labeled or identified as "confidential"), in any form or medium, disclosed to, developed or learned by him relating to the business, products, services, research or development of Motorola or its suppliers, distributors or customers.

273. Saxena has breached his agreements with Motorola by copying, using and/or disclosing Motorola confidential and proprietary information for purposes other than in the performance of his job duties for Motorola, and by retaining, using and disclosing Motorola confidential and proprietary information to Lemko and other third parties, and by working for Lemko during the term of his employment by Motorola without obtaining the prior approval of Motorola or disclosing the conflict of interest to Motorola.

274. Motorola has been injured by Saxena's breaches of the foregoing agreements.

WHEREFORE, Plaintiff, Motorola, Inc., respectfully requests that this Court enter the following relief against Defendant Saxena:

- a. enter judgment in favor of Motorola on Count Thirteen;
- b. award compensatory damages in an amount to be determined at trial
- c. order restitution and forfeiture of all compensation and benefits paid to Defendant Saxena by Motorola during the period of the breach of Defendant Saxena's loyalty to Motorola; and
- d. such further relief as this Court may deem just and proper, in law or equity.

COUNT FOURTEEN

TORTIOUS INTERFERENCE WITH CONTRACT

(Against Lemko)

275. Motorola repeats and realleges the averments of paragraphs 1-139, 188-274, as if fully set forth herein.

276. Throughout their employment at Motorola, Motorola maintained valid contractual relationships with Pan, Labun, Pyskir, Cai, Zhang and Favila in the form of their Employment Agreements and their agreement to abide by the Motorola Code of Conduct.

277. Motorola had a reasonable expectation that Defendants would fulfill their obligations under their agreements with Motorola.

278. Lemko knew of Defendants' contractual relationships with Motorola, but wrongfully and unjustifiably interfered with these relationships;

279. Lemko's interference caused Defendants to breach their agreements with Motorola by (1) disclosing confidential information of Motorola to Lemko; (2) assigning the property rights in inventions developed or conceived by Defendants when they were employed by Motorola to Lemko, and (3) working for Lemko, and (4) receiving compensation for services

from Lemko, without Motorola's prior consent and to the detriment of Defendants' job performance at Motorola.

280. Lemko's actions caused Defendants to breach their contractual relationships with Motorola.

281. Motorola has been injured by Lemko's actions.

WHEREFORE, Plaintiff, Motorola, Inc., respectfully requests that this Court enter the following relief against Defendants:

- a. enter judgment in favor of Motorola on Count Fourteen;
- b. award compensatory damages in an amount to be determined at trial;
- c. order disgorgement of all payments, revenue, profits, monies, royalties and any other benefits derived or obtained by Lemko from the breach of Defendants' fiduciary duties to Motorola;
- d. imposition of a constructive trust in favor of Motorola over all revenues or other benefits derived from the Lemko Patents or Patent Applications; and
- e. such further relief as this Court may deem just and proper, in law or equity.

COUNT FIFTEEN

FRAUDULENT CONCEALMENT

(Against Pan, Labun, Pyskir, Cai, Zhang, Favila and Saxena)

282. Motorola repeats and realleges the averments of paragraphs 1-139, as if fully set forth herein.

283. During the time that they were employed by Motorola, Defendants Pan, Labun, Pyskir, Cai, Zhang, Favila, Saxena and Jin were informed of and understood Motorola 's policy prohibiting them from working for a competitor of Motorola without Motorola's prior approval.

284. Defendants were further aware of and understood Motorola's policy requiring them to disclose to Motorola any situation that may have been or appeared to be a conflict of interest.

285. Defendants had a duty to disclose to Motorola that they were surreptitiously working for Lemko, diverting Motorola's confidential and proprietary information to Lemko, and devoting a substantial portion of their efforts to benefit Lemko rather than Motorola.

286. At no time during Defendants' employment at Motorola did they disclose the existence of Lemko to Motorola, nor did they disclose to Motorola the fact that they were diverting Motorola's confidential and proprietary information to Lemko, or that they were not working full-time for the benefit of Motorola or devoting their full and best efforts to Motorola.

287. Defendants' concealment of this information from Motorola was done knowingly and with the intent (a) that Motorola rely on the omission, (b) that Motorola would continue to believe that Defendants were working full time for Motorola, (c) that Motorola would continue to compensate Defendants with a full-time salary and benefits, and (d) that Motorola would continue to entrust Defendants with confidential and proprietary information of Motorola.

288. In reasonable reliance upon Defendants' omissions, Motorola continued to compensate Defendants with a full-time salary and benefits and entrusted them with confidential and proprietary information of Motorola.

289. Motorola was damaged as a result of Defendants' fraudulent concealment.

WHEREFORE, Plaintiff, Motorola, Inc. respectfully requests that this Court enter the following relief against Defendants:

- a. enter judgment in favor of Motorola on Count Fifteen;
- b. award compensatory damages in an amount to be determined at trial;
- c. award punitive damages in an amount sufficient to punish Defendants and deter such misconduct in the future;
- d. award Motorola the costs and attorneys' fees incurred in bringing this action; and
- e. such further relief as this Court may deem just and proper, in law or equity.

COUNT SIXTEEN**SPOLIATION OF EVIDENCE²****(Against Pan, Wu and Lemko)**

290. Motorola repeats and realleges the averments of paragraphs 1-139, as if fully set forth herein.

291. Defendants were aware of the claims made in this lawsuit at least by September 23, 2008, when they were served with the summons and complaint.

292. Defendants had a duty to exercise ordinary care to preserve the integrity of evidence that they knew or should have known would be material to the underlying causes of action in the complaint.

293. On May 26, 2009, the Court ordered Defendants to report to counsel for Motorola whether four computers named PANDELLM2, JAYPAN, JAY2 and D3RBDM8 could be delivered to Motorola's forensic experts for electronic imaging and further ordered the parties to work out the language of an order for the imaging of these four computers.

294. On May 27, 2009, Defendants reported to the Court that the computer named D3RBDM8 could not be located, and the Court entered an order requiring Defendants to deliver the PANDELLM2, JAYPAN, and JAY2 computers for electronic imaging by Motorola's forensic experts by 5:00 p.m. on May 28, 2009.

295. The PANDELLM2, JAYPAN, and JAY2 computers belonged to Defendant Pan and/or Defendant Wu and/or Defendant Lemko.

² Count Sixteen for Spoliation of Evidence was dismissed pursuant to the Court's Memorandum Opinion and Order dated April 12, 2010 (Dkt. 403) for failure to state a claim because the contentions were premature given the fact that discovery was at a fairly early stage. Plaintiff recognizes the Court's ruling as current law of the case, but repleads Count Sixteen in this Third Amended Complaint order to preserve the issue.

296. Defendants knew or should have known that information on the PANDELLM2, JAYPAN, and JAY2 computers was material to the underlying causes of action.

297. Notwithstanding their duty to preserve evidence, Defendants Pan and/or Defendant Wu intentionally and deliberately destroyed evidence on the computers by deleting files residing on the computer with an Eraser program and by tampering with the computer names and clocks.

298. Specifically, in the days and hours between the court's oral preservation order and the time that Defendants Pan and Lemko delivered the three computers for forensic imaging, the secure deletion program "Eraser" was used to delete and overwrite information from two of the three computers that were forensically imaged pursuant to court order.

299. Additionally, in the hours before the computers were to be turned over, elaborate changes were made to all three of the computers' clocks and the names of two of the computers in an apparent attempt to conceal evidence and/or the destruction of evidence.

300. But for the destruction of this evidence, Motorola had a greater probability of succeeding in the underlying lawsuit for, inter alia, violations of the Computer Fraud and Abuse Act and trade secret misappropriation.

301. Defendants' deliberate destruction of the evidence negatively affects Motorola's ability to prove otherwise valid claims for trade secret misappropriation and Computer Fraud and Abuse Act violations.

302. As a direct and proximate result of Defendants' destruction and/or modification of evidence, Motorola has been injured in that its ability to prosecute and enforce its legal rights against Defendants has been irrevocably prejudiced.

WHEREFORE, Plaintiff, Motorola, Inc., respectfully requests that this Court enter the following relief against Defendants Pan, Wu and Lemko:

- a. enter judgment in favor of Motorola on Count Sixteen;
- b. award compensatory damages in an amount to be determined at trial;
- c. award punitive damages in an amount sufficient to punish Defendants and deter such misconduct in the future; and
- d. such further relief as this Court may deem just and proper, in law or equity..

COUNT SEVENTEEN

COPYRIGHT INFRINGEMENT

(Against Lemko)

303. Motorola repeats and realleges the averments of paragraphs 1-139, as if fully set forth herein.

304. Motorola's source code is an original work of authorship and comprises copyrightable subject matter under the copyright laws of the United States, 17 U.S.C. §§ 101 *et seq.*

305. Motorola has complied in all respects with all laws governing copyright and has secured the exclusive rights and privileges in and to the copyrights for the aforementioned source code, as follows:

- Motorola received from the Registrar of Copyrights U.S. Copyright Registration No. TXU 1-621-667, which was registered on November 17, 2009. A true and correct copy of this Certificate of Registration is attached hereto as **EXHIBIT C**.
- Motorola received from the Registrar of Copyrights U.S. Copyright Registration No. TXU 1-636-373, which was registered on February 19, 2010. A true and correct copy of this Certificate of Registration is attached hereto as **EXHIBIT D**.

- Motorola received from the Registrar of Copyrights U.S. Copyright Registration No. TXu 1-641-780, which was registered on March 15, 2010. A true and correct copy of this Certificate of Registration is attached hereto as **EXHIBIT E**.
- Motorola received from the Registrar of Copyrights U.S. Copyright Registration No. TXu 1-645-268, which was registered on March 25, 2010. A true and correct copy of this Certificate of Registration is attached hereto as **EXHIBIT F**.

306. As the owner of the copyrights in the source code, Motorola enjoys the exclusive right to, among other things, reproduce the source code, prepare derivative works based on the source code, and distribute copies of the Motorola Site. *See 17 U.S.C. §§ 101, 106.*

307. Lemko has no rights in the copyrighted Motorola source code.

308. Lemko has infringed and continues to infringe said copyright, by copying the copyrighted Motorola source code, removing Motorola's copyright notice from the source code, and using the copyrighted source code as part of its own source code without Motorola's permission to do so.

309. Unless enjoined by this Court, Lemko will continue to infringe Motorola's copyright.

310. Lemko had access to the Motorola source code prior to creating the infringing Lemko source code.

311. At all times relevant hereto, Lemko has been aware or should have been aware of the existence of Motorola's exclusive rights in and to the copyrighted source code, and therefore, Lemko is a willful infringer of Motorola's copyright.

312. Motorola has been or is likely to be damaged by the acts of Lemko.

313. Motorola is entitled to recover from Lemko actual damages suffered by Motorola as a result of Lemko's infringement as well as Lemko's profits resulting from its infringement.

314. The infringement of Motorola' copyright by Lemko has caused, and will continue to cause, imminent irreparable harm to Motorola. Accordingly, Motorola is entitled to injunctive relief.

WHEREFORE, Plaintiff, Motorola, Inc., respectfully requests that this Court enter the following relief against Defendants:

- a. enter judgment in favor of Motorola on Count Seventeen;
- b. award damages in an amount to be determined at trial, including damages in the amount of Lemko's profits from its willful infringement of Motorola' copyrights;
- c. enter judgment that Lemko's copyright infringements have been knowing and willful;
- d. permanently enjoin Lemko, including its partners, officers, agents, servants, employees, parent, subsidiaries, sister companies, and all those persons and entities in active concert or participation with them, from further infringement of the copyrights in and to the Motorola source code, pursuant to 17 U.S.C. § 502;
- e. order the destruction of all source code or software, or copies thereof, made or used in violation of Motorola's exclusive rights, pursuant to 17 U.S.C. § 503; and
- f. such further relief as the Court may deem just and proper, in law or equity.

COUNT EIGHTEEN

CIVIL CONSPIRACY

(Against Pan, Labun, Pyskir, Cai, Zhang, Favila, Saxena, Jin, Howell, Vorick, Desai, Lemko and Huawei)

315. Motorola repeats and realleges the averments of paragraphs 1-139 and paragraphs 339-361, as if fully set forth herein.

316. Prior to July 2002, Defendants Howell, Labun, Pan and Pyskir, did each knowingly and willfully conspire and agree among themselves to commit wrongful acts damaging to Plaintiff Motorola, including: to breach, or to induce other Motorola employees to

breach, their contractual obligations and fiduciary duties to Motorola, by simultaneously working for the benefit of themselves and Lemko; to misappropriate Motorola's proprietary trade secrets and confidential information for the benefit of themselves and Lemko; to violate the Computer Fraud and Abuse Act by accessing Motorola's computers without authorization or exceeding their authorization in order to obtain valuable confidential and proprietary information of Motorola; to steal Motorola patents by means of filing applications for the benefit of Lemko on inventions that were invented by Motorola employees with a contractual obligation of assignment to Motorola; and to infringe Motorola copyrights for the benefit of themselves and Lemko.

317. Prior to August 2002, Defendant Vorick did join the aforementioned conspiracy, which is ongoing, and did knowingly and willfully conspire and agree with the aforementioned conspirators to commit wrongful acts enumerated above.

318. Prior to September 2002, Defendant Cai did join the aforementioned conspiracy, which is ongoing, and did knowingly and willfully conspire and agree with the aforementioned conspirators to commit wrongful acts enumerated above.

319. Prior to September 2002, Defendant Zhang did join the aforementioned conspiracy, which is ongoing, and did knowingly and willfully conspire and agree with the aforementioned conspirators to commit wrongful acts enumerated above.

320. Prior to December 2002, Defendant Desai did join the aforementioned conspiracy, which is ongoing, and did knowingly and willfully conspire and agree with the aforementioned conspirators to commit wrongful acts enumerated above.

321. Prior to June 2004, Defendant Saxena did join the aforementioned conspiracy, which is ongoing, and did knowingly and willfully conspire and agree with the aforementioned conspirators to commit wrongful acts enumerated above.

322. Prior to June 2004, Defendant Favila did join the aforementioned conspiracy, which is ongoing, and did knowingly and willfully conspire and agree with the aforementioned conspirators to commit wrongful acts enumerated above.

323. Prior to June 2004, Defendant Jin did join the aforementioned conspiracy, which is ongoing, and did knowingly and willfully conspire and agree with the aforementioned conspirators to commit wrongful acts enumerated above.

324. One or more of Defendants committed numerous overt acts in furtherance of the common scheme, including but not limited to unlawfully misappropriating Motorola's Trade Secret Information, and retaining such information after Defendants' employment with Motorola ended despite their prior agreements to return such property and despite Motorola's demand for the return of the property, using and transferring Motorola's Trade Secret Information for the benefit of Defendant Lemko, and copying and/or destroying Motorola's electronically stored information.

325. In particular, Defendant Howell's wrongful acts include: coordinating, scheduling, and arranging reimbursement for multiple business trips of Motorola employees Cai, Pan, Pyskir and Zhang for the benefit of Lemko, and making financial and business arrangements for Lemko, in furtherance of the conspiracy for the benefit of Lemko.

326. In particular, Defendant Labun's wrongful acts include: generating or assisting in the preparation of profit and loss spreadsheets, business plans and other Lemko documents, providing executive oversight of the formation and ongoing operations of Lemko while

employed at Motorola, and inducing his subordinates at Motorola to breach their fiduciary duties to Motorola and their agreements with Motorola, in furtherance of the conspiracy for the benefit of Lemko.

327. In particular, Defendant Pan's wrongful acts include: assigning inventions he invented while employed at Motorola to Lemko, working on Lemko engineering projects while employed at Motorola, transferring Motorola's proprietary trade secrets and confidential information to third parties including to Lemko personnel and to additional parties both within and outside the United States, making numerous business trips on behalf of Lemko both within and outside the United States, including China, while employed at Motorola, inducing his subordinates at Motorola to breach their fiduciary duties to Motorola and their agreements with Motorola, and inducing Defendant Wu and Defendant Bai to misappropriate Motorola's proprietary trade secrets and confidential information, in furtherance of the conspiracy for the benefit of Lemko.

328. In particular, Defendant Pyskir's wrongful acts include: generating or assisting in the preparation of business plans and other Lemko documents and providing executive oversight of the formation and ongoing operations of Lemko while employed at Motorola, making multiple business trips on behalf of Lemko both within and outside the United States, including China, while employed at Motorola, and inducing his subordinates at Motorola to breach their fiduciary duties to Motorola and their agreements with Motorola, in furtherance of the conspiracy for the benefit of Lemko.

329. In particular, Defendant Vorick's wrongful acts include: generating or assisting in the preparation of business plans and other Lemko documents, providing marketing expertise for

Lemko, and participating in business meetings for the benefit of Lemko with people she knew to be Motorola employees, in furtherance of the conspiracy for the benefit of Lemko.

330. In particular, Defendant Cai's wrongful acts include: working on Lemko engineering projects while employed at Motorola, providing technical expertise and demonstrations for customer, vendor or investor presentations for the benefit of Lemko while employed at Motorola, making multiple business trips on behalf of Lemko both within and outside the United States, including China, while employed at Motorola, and participating in the preparation of patent applications for the benefit of Lemko on inventions that were invented by Motorola employees with a contractual obligation of assignment to Motorola, in furtherance of the conspiracy for the benefit of Lemko.

331. In particular, Defendant Zhang's wrongful acts include: working on Lemko engineering projects while employed at Motorola, providing technical expertise and demonstrations in customer, vendor or investor presentations for the benefit of Lemko while employed at Motorola, making multiple business trips on behalf of Lemko both within and outside the United States, including China, while employed at Motorola, and participating in the preparation of patent applications for the benefit of Lemko on inventions that were invented by Motorola employees with a contractual obligation of assignment to Motorola, in furtherance of the conspiracy for the benefit of Lemko.

332. In particular, Defendant Desai's wrongful acts include: generating or assisting in the preparation of business plans and other Lemko documents and providing business development expertise for Lemko, coordinating and scheduling multiple business trips of Motorola employees Cai, Pan, Pyskir and Zhang for the benefit of Lemko, and participating in

business meetings for the benefit of Lemko with people he knew to be Motorola employees, in furtherance of the conspiracy for the benefit of Lemko.

333. In particular, Defendant Saxena's wrongful acts include: working on Lemko engineering projects that included Motorola's proprietary trade secrets and confidential information while employed at Motorola, including the installation and operation of a Lemko trial site in Colombia, in furtherance of the conspiracy for the benefit of Lemko.

334. In particular, Defendant Favila's wrongful acts include: working on Lemko engineering projects that included Motorola's proprietary trade secrets and confidential information while employed at Motorola, including the installation and operation of a Lemko trial site in Colombia, in furtherance of the conspiracy for the benefit of Lemko.

335. In particular, Defendant Jin's wrongful acts include: working on Lemko engineering projects while employed at Motorola and transferring Motorola's proprietary trade secrets and confidential information to third parties including to Lemko personnel and to additional parties both within and outside the United States, including China, in furtherance of the conspiracy for the benefit of Lemko.

336. As a direct result of the foregoing conduct and the conduct alleged in paragraphs 339-361, which are incorporated herein by reference, Defendants have caused and continue to cause damage to Motorola, including but not limited to attorneys' fees and costs that have been expended and that will be expended in the future by Motorola to enforce its legal rights.

337. Defendants' conduct was willful and malicious and performed with an evil motive and with reckless indifference to the rights of others, entitling Motorola to punitive damages.

WHEREFORE, Plaintiff, Motorola, Inc., respectfully requests that this Court enter the following relief against Defendants:

- a. enter judgment in favor of Motorola on Count Eighteen;
- b. award compensatory damages in an amount to be determined at trial;
- c. award punitive damages in an amount sufficient to punish Defendants and deter such misconduct in the future;
- d. award Motorola the costs and attorneys' fees incurred in bringing this action; and
- e. such further relief as this Court may deem just and proper, in law or equity.

COUNT NINETEEN

**THREATENED OR ACTUAL
MISAPPROPRIATION OF TRADE SECRETS**

(Against Huawei)

338. Motorola repeats and realleges the averments of paragraphs 1-139, as if fully set forth herein.

339. The Motorola proprietary trade secrets and confidential information, set forth individually and collectively in the preceding paragraphs of the Complaint, are statutory "trade secrets" protected by the Illinois Trade Secrets Act, 765 ILCS 1065/1 et seq.

340. At all times, Motorola has taken reasonable measures to protect the Motorola proprietary trade secrets and confidential information, and Motorola derives economic value and competitive advantage from such information not being generally known to the public or trade.

341. Defendant Huawei was founded by Ren Zhengfei, a former officer in the People's Liberation Army (PLA) in 1988 and within just 20 years has emerged as China's largest telecommunications vendor and as one of the world's largest mobile network suppliers. Huawei is a direct and major competitor of Motorola in the United States and around the world.

342. Defendant Shaowei Pan met with Ren Zhengfei, the founder and chairman of Huawei, in Beijing in 2001 but the details of this meeting have not been discovered yet from the limited evidence obtained from discovery in this litigation to date. However, it is established

that in 2001 and at all times up to and including April 2, 2004, Defendant Shaowei Pan was a trusted senior engineer and director of architecture working full time at Motorola on the development of new products and new technologies for Motorola. However, as set forth below, Defendant Shaowei Pan and the other defendants secretly were engaged in new product development for Huawei.

343. Defendants Shaowei Pan, Labun, Pyskir, Cai and Zhang were working at Motorola on the proprietary “Seamless Mobility” initiative in 2001 and one of the critical requirements for this initiative was the availability of the Motorola SC300 base station transceiver (BTS). The revolutionary Motorola SC300 BTS was called a “microcell” and it was very small and compact and weighed only 53 pounds. The Motorola SC300 BTS, together with the “Seamless Mobility” technology initiatives of All-IP and soft-switching solutions, now opened up opportunities for cellular applications in rural areas, in-building cellular systems, urban shopping malls, mobile cellular systems and emergency disaster zones because the Motorola SC300 BTS was small and portable and could easily be attached to poles, walls, vehicles and other structures. With proprietary GPS, Bluetooth and other proprietary technologies, there were various configurations being developed by Motorola to create an “instant cellular” system utilizing Motorola SC300 “microcells.”

344. Defendant Huawei did not have a BTS comparable to the Motorola SC300 in 2001.

345. In or about August 24, 2002, Defendant Shaowei Pan reported to Ren Zhengfei at Huawei that “we have developed some products in our spare time” and “we did some market investigations and contacted some Brazilian and Indian customers.” The report to Huawei founder and chairman Ren Zhengfei on the result of these market investigations: “They were

very interested in these products.” At all times during these 2001-2002 activities, Huawei acting in concert with Defendant Shaowei Pan and other defendants knew or had reason to know that these “products” and proprietary technologies being developed by Defendant Shaowei Pan and others for the benefit of Huawei involved the unauthorized acquisition, disclosure and use of Motorola proprietary trade secrets and confidential information and Motorola resources.

346. Shaowei Pan also reported to Ren Zhengfei on or about August 24, 2002: “If our plan can progress smoothly, Lemko will be the company we are planning to establish, and it will be independent of Motorola, Inc.”

347. Arrangements were made for Defendant Shaowei Pan to travel to China and “[we] will take some products with us for presentation.” These presentations were to include: “IP mobile control and switches, Bluetooth and CDMA cellular mobile voice communication and Bluetooth cellular data communication.” This trip was scheduled in September 2002. Huawei knew or should have known that the “products” and proprietary technology being brought to China for “presentation” to the founder and chairman of Huawei were acquired and derived from misappropriated Motorola trade secrets and confidential information by full time Motorola employees.

348. Defendant Shaowei Pan purchased three tickets to China for a visit from February 15, 2003 to March 2, 2003 for himself, Defendant Hechun Cai, and Defendant Jinzhong Zhang.

349. Upon information and belief, much of the evidence of the secret business relationship between Huawei, Defendant Shaowei Pan, Lemko and the other defendants was destroyed when Defendant Shaowei Pan ran file destruction software on his home computers after Defendant Pan and Lemko were ordered by the Court to turn over Pan’s home computers by 5 p.m. on May 28, 2009, and just before the computers were actually turned over.

350. However, there is at least part of an email chain that has been recovered that confirms that Defendant Shaowei Pan, at Huawei's request, transmitted proprietary and confidential Motorola specifications for the Motorola SC300 base station to Ren Zhengfei and JinLong Hou, Huawei's vice president of wireless communications, in March 2003 and that a meeting and an agreement for the transfer of Motorola proprietary information did in fact take place in Beijing during the China trip in February-March 2003.

351. On March 3, 2003, immediately upon Defendant Pan's return to the United States, a recovered email shows that Shaowei Pan using his private email account, and at Huawei's request, did in fact transfer Motorola's proprietary and confidential specifications for the Motorola SC300 base station to JinLong Hou and Ren Zhengfei. The Motorola proprietary information sent by Shaowei Pan is described in the email chain by Shaowei Pan as "Attached please find those document about SC300 (CDMA 2000 1X) specification you asked."

352. On March 3, 2003, JinLong Hou acknowledged receipt of these proprietary Motorola SC300 specifications on behalf of Huawei. The Motorola SC300 specifications have been recovered from Defendant Pan's computer and the Motorola specification sent to Huawei by Defendant Shaowei Pan is marked "Motorola Confidential Proprietary" on the front page of the specification and every page of the specification.

353. Other Motorola proprietary trade secrets and confidential information have been recovered from computers produced pursuant to Court Order on May 28, 2009 including proprietary information from Motorola labs, various proprietary technical specifications, proprietary Motorola implementation specifications and requirements, proprietary system architecture, proprietary functional requirement documentation for the Motorola SuperCell (SC) system, detailed Motorola proprietary functional system descriptions, proprietary technical

requirement documents, proprietary Motorola source code documents and, upon information and belief, much if not all of this information has been disclosed, used and transmitted by the defendants to Huawei and Lemko without Motorola's authorization and consent.

354. The recovered email chain showing the transmission of Motorola proprietary SC300 specifications to Huawei marked "Motorola Confidential Proprietary" by Shaowei Pan from a private email account establishes that Huawei and its officers knew they were receiving stolen Motorola proprietary trade secrets and confidential information without Motorola's authorization and consent.

355. The business relationship between Lemko and Huawei remains under investigation but one document recovered from one of the computers ordered to be produced by Court Order shows a creation date of May 18, 2002; a last saved date of March 1, 2004 and a title called "OEM Agreement." This "OEM Agreement" document lists Chen Zhongyuan (Huawei) and Shaowei Pan (Lemko) as the "Executive Interface" contacts; Ren Bo (Huawei) and Bo Pyskir (Lemko) as the "Product Management" contacts; Zhang Zhenjun (Huawei) and Nick Desai (Lemko) as the "Domestic Marketing Management" contacts; Tang Feng (Huawei) and Faye Vorick (Lemko) as the "Overseas Marketing Management" contacts; Li Xianyong (Huawei) and Jinzhong Zhang (Lemko) as the "Support Services Management" contacts; Wang Kefeng (Huawei) and Hechun Cai (Lemko) as the "Repair/Replacement Interface" contacts; Wu Shengfei (Huawei) and Shaowei Pan (Lemko) as the "Document Representatives" contacts; Xia Zhihui (Huawei) and Ray Howell (Lemko) as the "Commercial" contacts; and Hou Linlin (Huawei) and Paul Gilman (Lemko) as the "Legal" contacts.

356. The technology that Lemko was developing jointly with Huawei with the secret involvement of full time Motorola employees and engineers, including Defendants Shaowei Pan,

Nicholas Labun, Bo Pyskir, and former Motorola employees, Ray Howell and Faye Vorick in the 2002-2004 time period has been described as “distributed mobile architecture” (DMA) and alternatively as a “control and soft switch element” (CASSE). This technology at all times was developed with purloined Motorola proprietary trade secrets and confidential information and is derived from the “Seamless Mobility” initiative that Defendant Pan and the other defendants were working on at Motorola.

357. The DMA/CASSE system replaces the functions of the Base Station Controller (BSC) and Mobile Switching Center (MSC) and is available for CDMA, GSM and UMTS applications. At all times, the research and development of the DMA/CASSE system by Lemko, in concert with Huawei, did in fact involve misappropriated Motorola proprietary trade secrets and confidential information as well as the assistance of full time Motorola engineers and others named as Defendants in this action. At all times, Huawei knew that the “test” systems and “trial” systems including prototypes sent to China in 2002 and 2003 were built and derived from Motorola proprietary trade secrets and confidential business information with the involvement of full time Motorola employees.

358. Defendants Shaowei Pan and Huawei identified various potential markets for the DMA/CASSE “instant cellular network” system utilizing a Huawei BTS and the DMA/CASSE system and described as a complete and self-contained cellular system that replicates the functionality of a cellular switch, base station controller and transceiver with applications including the installation on military vehicles, wireless local loops, in building cellular systems, disaster zones and rural areas.

359. Defendants Lemko and Huawei have been testing, demonstrating and selling these misappropriated technologies in the United States and all over the world. Defendant Angel

Favila and others, including Defendant Shaowei Pan, have made several trips to work with Huawei on the DMA/CASSE technologies at FutureWei, Huawei's wholly-owned subsidiary located in Dallas, Texas.

360. Both Lemko and Huawei are now marketing and selling DMA/CASSE cellular "solutions" in separate channels. Lemko uses the moniker "Node 1, Node 2 and Node 3" solutions and such other marketing terms as an "All-IP" network and "On Demand Cellular" solutions. Huawei, in turn, is marketing the DMA/CASSE base station "solution" as the "EasyGSM BTS", described as "the industry's first all IP-based compact BTS" that can be "mounted on a pole, wall, or tower," and under other trade names including the 3600 series, 3900 series and 6900 series products. All of these Lemko/Huawei "solutions" and "products" can be traced back to the same all-IP and/or soft-switching characteristics of the Motorola Seamless Mobility technology and the proprietary SC300 microcell BTS in 2001 when the Lemko/Huawei relationship was secretly formed and from which these solutions and products were created and derived from purloined Motorola proprietary trade secrets and confidential information without Motorola's knowledge or consent.

361. All of the actions by Huawei in concert with the Defendant Shaowei Pan, Lemko and the other defendants, as set forth in the preceding paragraphs constitutes the willful and malicious misappropriation of Plaintiff's proprietary trade secrets and confidential information and entitles Motorola to exemplary damages and an award of attorneys' fees and costs pursuant to the Illinois Trade Secrets Act, 765 ILCS 1065/1 et seq.

WHEREFORE, Plaintiff, Motorola, Inc., respectfully requests that this Court enter the following relief against Defendant:

- a. judgment in favor of Motorola on Count Nineteen;

- b. both preliminary and permanent relief pursuant to 765 ILCS 1065/1, et seq. restraining and enjoining Defendant Huawei, its officers, directors, employees, agents, and all those in privity, concert or participation with it from the threatened or actual misappropriation of the Motorola proprietary trade secrets and confidential information;
- c. a finding that Defendant Huawei's acts and conduct constitute the actual or threatened misappropriation of trade secrets in violation of 765 ILCS 1065/1, et seq., and that such acts and conduct are and have been willful and malicious;
- d. compensatory and increased damages sustained as a result of Defendant Huawei's wrongful actions, together with an accounting of Defendants' profits and unjust enrichment arising from such actions;
- e. an order compelling Defendant Huawei to return any and all of Plaintiff's proprietary trade secrets and confidential information including all types of scientific, technical and engineering information, files, documents, drawings, schematics, programs, object code, source code, designs, prototypes and the like, in Defendants' possession, custody or control, and wherever and however stored physically, electronically, graphically, photographically, or in writing, and all derivations and compilations and/or other memorializations of such purloined information; together with such other affirmative relief required to compel compliance with this order, including the use of electronic evidence experts and other technicians;
- f. an order compelling Defendant Huawei to disclose its actual and potential customers and any and all persons and entities to which Defendant Huawei disclosed Plaintiff's proprietary trade secrets and confidential information;
- g. attorneys' fees and costs pursuant to 765 ILCS 1065/1, et seq.; and such further relief as this Court may deem just and proper, in law or equity.

JURY DEMAND

Pursuant to FED. R. CIV. P. 38(b), Motorola respectfully demands a trial by jury of all issues triable by a jury in its Complaint.

* * *

Date: July 16, 2010

Respectfully submitted,

/s/ R. Mark Halligan

R. Mark Halligan (IL 6200723)

rmhalligan@nixonpeabody.com

Deanna R. Swits (IL 6287513)

dswits@nixonpeabody.com

Jodi Rosen Wine (IL 6209883)

jwine@nixonpeabody.com

Jason T. Kunze (IL 6300271)

jkunze@nixonpeabody.com

NIXON PEABODY LLP

300 South Riverside Plaza, 16th Floor

Chicago, IL 60606

Tel: 312-425-3900

Fax: 312-425 3909

Attorneys for Plaintiff Motorola, Inc.

**EXHIBIT A
TO
THIRD AMENDED COMPLAINT**



MOTOROLA

EMPLOYMENT AGREEMENT

In consideration of my employment, or continued employment by Motorola, Inc. or its subsidiaries (referred to separately or together as "Motorola") and the salary or wages paid to me, I understand and agree to the following provisions for the protection of Motorola property rights:

1. Not to disclose to Motorola, or to use in my work at Motorola (a) any confidential information belonging to others, including my prior employers (unless written authorization is first obtained), or (b) any prior inventions made by me which Motorola is not otherwise entitled to learn of or to use.

2. Not to use, or to publish, or to otherwise disclose to others, either during or subsequent to my employment by Motorola, any confidential information of Motorola (including confidential information of customers and suppliers), except as my Motorola duties may require.

3. Upon termination of my employment by Motorola, to promptly deliver to a designated Motorola representative all documents and other records which relate to the business activities of Motorola, or any other materials which belong to Motorola.

4. To assign and I hereby assign to Motorola as its exclusive property the entire right, title and interest in all my inventions, innovations, or ideas developed or conceived by me solely, or jointly with others, at any time during the term of my employment and which inventions, innovations, or ideas relate to the actual or anticipated business activities of Motorola, or result from, or are suggested by, work which I do for Motorola.

5. To make and maintain written records of all inventions, innovations, or ideas referred to in paragraph 4 above and to submit promptly such records, and supplemental oral disclosures, to designated representatives of Motorola.

6. To execute all papers, and otherwise provide proper assistance, at Motorola's request and expense, during and subsequent to my employment by Motorola to enable Motorola or its nominees to obtain patents, copyrights, and legal protection for inventions or innovations in any country.

7. I represent that the inventions identified in the _____ pages I attach hereto comprise all the unpatented inventions which I have made or conceived prior to my employment by Motorola, which inventions shall be excluded from this agreement. (It is only necessary to list the title of such inventions and the purpose thereof, but not details of the invention itself per paragraph 1(b)). IF THERE ARE NO SUCH UNPATENTED INVENTIONS TO BE EXCLUDED, EMPLOYEE INITIAL HERE _____.

8. I further represent that I have attached hereto a copy of any agreement which presently affects my compliance with the terms of this present agreement. (Such copy must specify the other contracting party or employer, the date of such agreement, the date of termination of any employment). IF THERE IS NO SUCH AGREEMENT, EMPLOYEE INITIAL HERE _____.

This agreement replaces any existing employee agreement between Motorola and me regarding patents and/or confidential information and shall be binding on my executors, administrators, heirs, legal representatives or assigns.

This agreement may not be modified except in writing with approval of an officer of Motorola.

WITNESS	EMPLOYEE
SIGNATURE	SIGNATURE
TYPED OR PRINTED NAME	TYPED OR PRINTED NAME
DATE	SOCIAL SEC. NO. DATE

**EXHIBIT B
TO
THIRD AMENDED COMPLAINT**

EMPLOYEE CONFIDENTIALITY AND ASSIGNMENT OF INVENTIONS AGREEMENT

THIS EMPLOYEE CONFIDENTIALITY AND ASSIGNMENT OF INVENTIONS AGREEMENT ("Agreement") is made by the undersigned employee ("I" or "me") with Motorola, Inc. ("Motorola"). Motorola includes its successors, assigns, current and former affiliates ("affiliates" defined to mean entities that own, are owned by, or are under common ownership with Motorola, Inc.). In consideration of my employment by Motorola and other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, I agree as follows:

1. NONDISCLOSURE OF CONFIDENTIAL INFORMATION

Definitions: As used in this Agreement, "Confidential Information" means all confidential information and trade secrets (whether or not specifically labeled or identified as "confidential"), in any form or medium, that is disclosed to, or developed or learned by me and that relates to the business, products, services, research or development of Motorola or its suppliers, distributors or customers and that has not become publicly known. As used in this Agreement, Confidential Information includes all "Intellectual Property", which means all patent applications, ideas, inventions, formulae, know-how, devices, designs, models, methods, techniques and processes, specifications, tooling, computer programs, copyrightable works, mask works, technical and product information concerning circuits, and all other intellectual property rights.

I recognize that Motorola is engaged in a continuous program of research and development, and that as an employee, I will have access to Confidential Information that has independent economic value to Motorola in part because it is confidential. I further recognize that Motorola has taken reasonable steps to protect its Confidential Information from disclosure to the public, including entering into this Agreement. During and after my employment, I will not disclose or use any Confidential Information except to the extent I am required to disclose or use such Confidential Information in the performance for my assigned duties; and I will use my best efforts to safeguard the Confidential Information and protect it against disclosure, misuse, espionage, loss and theft. In the event Motorola has entered into confidentiality agreements, which contain provisions different from and more restrictive than those set forth in this Agreement, I agree to comply with any such different and more restrictive provisions of which I am notified. Confidential Information or Intellectual Property of third parties, including my former employers, may have been disclosed to me and I lawfully may be bound not to disclose such information to others. I agree not to disclose such information or violate such nondisclosure restrictions and agree to provide Motorola with copies of any written agreements with former employers that contain such restrictions.

2. OWNERSHIP OF INTELLECTUAL PROPERTY

I hereby assign and agree to assign to Motorola all right, title and interest that I may have or acquire in and to any Intellectual Property that relates in whole or in part to Motorola's business or actual or demonstrably anticipated research or development, to the extent such Intellectual Property is not already owned by Motorola as a matter of law. I shall reduce to writing any Intellectual Property not already in such form and promptly and fully communicate to Motorola all such Intellectual Property and I shall, both during and after my employment, cooperate with Motorola, at its reasonable expense, to protect Motorola's interests in such Intellectual Property. In the event that Motorola is unable to secure my signature to any document required for any application process for such Intellectual Property, I hereby irrevocably appoint Motorola and its duly authorized officers and agents, as my agents and attorneys-in-fact, to act on my behalf to do any lawfully permitted acts to further the prosecution or issuance of patents for such Intellectual Property with the same legal effect as if executed by me.

I hereby irrevocably waive any and all "moral rights" that I may have in the Intellectual Property created hereunder (the "Work Product"), or any part thereof, in connection with Motorola's use(s) thereof. To the extent such waiver may be unenforceable, I agree that I will, without further remuneration (except for out-of-pocket expenses), execute and deliver to Motorola such waiver of my moral rights concerning the Work Product and Motorola's use(s) thereof. I acknowledge and understand that the term "moral rights" as used herein includes the right of an author to be known as the author of his/her work to prevent others from being named as the author of his/her work to prevent

others from making deforming changes in his/her work and to prevent others from using the work or the author's name in such a way as to reflect negatively on his/her professional standing.

During the term of my employment with Motorola and for a period of six (6) months after termination, I will promptly disclose to Motorola all Intellectual Property, that relates in whole or in part to Motorola's business or actual or demonstrably anticipated research or development, and that is created, conceived or reduced to practice by me, either alone or jointly with others, whether or not patentable or subject to copyright. I acknowledge and agree that any Intellectual Property related to Motorola's business or research or development, and that is created, conceived or reduced to practice by me (whether alone or jointly with others) within six (6) months after termination of my employment with Motorola will be presumed to have been conceived or made during the period of my employment with Motorola, unless and until established to the contrary by me. I hereby assign such Intellectual Property to Motorola.

I agree that this Agreement does not require assignment of any of my rights in an invention if I can establish that: no equipment, supplies, facilities or Confidential Information of Motorola were used; the invention was developed entirely on my own time and did not result from any work performed by me for Motorola; or that the invention does not relate, at the time of conception or reduction to practice, to Motorola's business or its research or development. I acknowledge and agree that any materials, authored, prepared, contributed to or written by me, in whole or in part, shall be done as "work made for hire" as defined and used in the Copyright Act of 1976, 17 U.S.C. § 101, et seq. Prior to my employment at Motorola, I did not make or acquire any interest in inventions, that are the subject of issued patents or pending patent applications, or that might become the basis for one or more patent applications, other than those listed on Exhibit A.

3. OWNERSHIP AND RETURN OF MATERIALS

All documents and materials, which I have had access to or produced in connection with my services for Motorola, or which belong to Motorola, whether or not such materials contain Confidential Information, shall remain the sole property of Motorola. Upon termination, or at any time requested, I shall promptly deliver to Motorola all such materials and copies in my possession and control and shall provide written confirmation that I have returned all such materials.

4. NON-SOLICITATION BY EMPLOYEE

In further consideration of my employment by Motorola, I agree that during the term of my employment with Motorola and for a period of twelve (12) months after termination of my employment with Motorola, I shall not, directly or indirectly, induce or attempt to induce (i) any employee of Motorola or any of its subsidiaries or affiliates to leave the employ of Motorola or such subsidiary or affiliate or (ii) any other person to terminate a relationship with Motorola or any of its subsidiaries or affiliates. To the extent that any other agreements that I previously have entered into, or may enter into in the future, with Motorola contain provisions regarding my non-solicitation obligations that are different than or more restrictive than those set forth in this Agreement, I agree to comply with any such different and more restrictive provisions to which I have agreed.

5. NONCOMPLIANCE

I acknowledge and agree that the limitations set forth herein are reasonable with respect to scope, and duration, and are properly required for the protection of the legitimate business interest of Motorola. I acknowledge that my compliance with this Agreement is necessary to protect Motorola's goodwill and Confidential Information, that my failure to comply with this Agreement will irreparably harm the business of Motorola, and that monetary damages would not provide an adequate remedy to Motorola in the event of such non-compliance. Therefore, Motorola shall be entitled to obtain an injunction and other equitable relief in any court of competent jurisdiction against a breach by me of this Agreement, without the posting of bond or other security, in addition to whatever other remedies it may have. I agree that any action relating in any way to this Agreement shall be brought solely in a court of competent jurisdiction for the location of the Motorola facility at which I worked and consent to the jurisdiction of any such court and hereby waive any defense or objection related to improper or inconvenient forum, venue

or jurisdiction. In the event that Motorola successfully enforces this Agreement against me in any court, I will indemnify Motorola for the actual costs incurred by Motorola in enforcing this Agreement, including but not limited to attorneys' fees.

6. EMPLOYEE AT WILL

This Agreement does not constitute an employment agreement and I understand that I remain an employee at will. This means that I may resign at any time and Motorola may terminate my employment at any time, with or without cause and with or without notice.

7. MISCELLANEOUS

This Agreement shall be governed by, and construed and interpreted in accordance with the laws of Illinois (or if I am employed outside of the United States, the applicable local legal jurisdiction for the location of the Motorola facility at which I worked) without regard to conflict of law principles.

I agree that Motorola may present a copy of this Agreement to any of my actual or prospective subsequent employers. I also agree that upon termination and for a period of 12 months thereafter, I will immediately inform Motorola of the identity of any subsequent employer, my new position and job duties and responsibilities and any other information necessary to determine my compliance with the terms of this Agreement.

Any waiver by Motorola of the breach of or its right to enforce any provision of this Agreement shall not operate or be construed as a waiver of any subsequent breach or right of enforcement. The provisions of this Agreement are severable; if any provision is found to be unenforceable, the remaining provisions shall remain in full force and effect. If the scope of any provision in this Agreement is found to be too broad to permit its full enforcement, I consent to judicial modification of such provision and enforcement to the maximum extent permitted by law.

This Agreement and Exhibit A attached to this Agreement contain the entire agreement between the parties with respect to the subject matter hereof and supersede any previous understandings or agreements, whether written or oral, by or between the parties. No amendment to this Agreement, and no waiver of any one or more of the provisions of this Agreement, shall be effective unless set forth in writing and signed by the parties hereto.

8. UNDERSTAND AGREEMENT

I REPRESENT AND WARRANT THAT: (A) I HAVE READ AND UNDERSTAND THIS AGREEMENT; (B) I HAVE HAD THE OPPORTUNITY TO OBTAIN ADVICE FROM LEGAL COUNSEL OF MY CHOICE IN ORDER TO INTERPRET THIS AGREEMENT; AND (C) I HAVE BEEN GIVEN A COPY OF THIS AGREEMENT.

IN WITNESS WHEREOF, I acknowledge that this Agreement is neither a contract of employment nor a guarantee of continued employment and, intending to be legally bound hereby, I have executed this Agreement this _____ day of _____, 20____.

Signature: _____

Full Name: _____

Employee ID No. (i.e., Social Security #, government ID #, Motorola Commerce ID): _____

EXHIBIT A

TO THE

**EMPLOYEE CONFIDENTIALITY
AND ASSIGNMENT OF INVENTIONS AGREEMENT**

The following is a complete list of all inventions or improvements or works of authorship or other Intellectual Property relevant to the subject matter of my employment with, and/or the business of, Motorola, Inc. ("Motorola") that have been made or conceived or first reduced to practice by me alone or jointly with others prior to my employment by Motorola.

- No inventions, improvements, works of authorship or other Intellectual Property.
- See below.
- Additional sheets attached.

DATE: _____

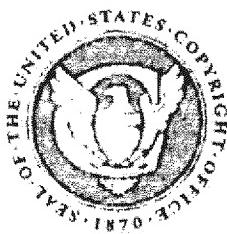
Signature: _____

Full Name: _____

Employee ID No. (i.e., Social Security #, government ID #, Motorola Commerce ID): _____

**EXHIBIT C
TO
THIRD AMENDED COMPLAINT**

Certificate of Registration



This Certificate issued under the seal of the Copyright Office in accordance with title 17, *United States Code*, attests that registration has been made for the work identified below. The information on this certificate has been made a part of the Copyright Office records.



Marybeth Peters
Register of Copyrights, United States of America

Registration Number
TXu 1-621-667

Effective date of
registration:
November 17, 2009

Title _____

Title of Work: userMagicCookies.hh

Completion/ Publication _____

Year of Completion: 2001

Author _____

■ Author: Motorola, Inc.

Author Created: text and editing of computer program

Work made for hire: Yes

Citizen of: United States

Domiciled in: United States

Year Born: 1928

Copyright claimant _____

Copyright Claimant: Motorola, Inc.

1303 East Algonquin Road, Schaumburg, IL, 60196, United States

Rights and Permissions _____

Organization Name: Motorola, Inc.

Telephone: 847-576-5000

Address: 1303 East Algonquin Road

Schaumburg, IL 60196 United States

Certification _____

Name: Jason T. Kunze

Date: November 14, 2009

Correspondence: Yes

Registration #: TXU001621667

Service Request #: 1-281706956

Nixon Peabody LLP
Jason T Kunze
300 S. Riverside Suite 1600
Chicago, IL 60606-6613 United States

**EXHIBIT D
TO
THIRD AMENDED COMPLAINT**

Certificate of Registration



This Certificate issued under the seal of the Copyright Office in accordance with title 17, *United States Code*, attests that registration has been made for the work identified below. The information on this certificate has been made a part of the Copyright Office records.

Marybeth Peters

Register of Copyrights, United States of America

Registration Number
TXu 1-636-373

Effective date of
registration:
February 19, 2010

Title

Title of Work: CcBaseMsg.hh

Completion/Publication

Year of Completion: 2001

Author

- Author: Motorola Inc.
- Author Created: text, editing, computer program
- Work made for hire: Yes
- Citizen of: United States
- Year Born: 1928

Domiciled in: United States

Copyright claimant

Copyright Claimant: Motorola Inc.
1303 East Algonquin Road, Schaumburg, IL, 60196, United States

Rights and Permissions

Organization Name: Motorola Inc.
Telephone: 847-576-5000
Address: 1303 East Algonquin Road
Schaumburg, IL 60196 United States

Certification

Name: Jason T. Kunze
Date: February 16, 2010
Applicant's Tracking Number: 049423.001000

Registration #: TXU001636373

Service Request #: 1-340141034

Nixon Peabody LLP
Jason T. Kunze
300 South Riverside Plaza Suite 1600
Chicago, IL 60606-6613 United States

**EXHIBIT E
TO
THIRD AMENDED COMPLAINT**

Certificate of Registration



This Certificate issued under the seal of the Copyright Office in accordance with title 17, *United States Code*, attests that registration has been made for the work identified below. The information on this certificate has been made a part of the Copyright Office records.

Register of Copyrights, United States of America

Registration Number

TXu 1-641-780

Effective date of
registration:

March 15, 2010

Title

Title of Work: **rtpTypes.h**

Completion/Publication

Year of Completion: 2001

Author

Author: Motorola Inc.

Author Created: Editing, computer program

Work made for hire: Yes

Citizen of: United States

Domiciled in: United States

Year Born: 1928

Copyright claimant

Copyright Claimant: Motorola Inc.

1303 East Algonquin Road, Schaumburg, IL, 60196, United States

Rights and Permissions

Organization Name: Motorola Inc.

Telephone: 847-576-5000

Address: 1303 East Algonquin Road

Schaumburg, IL 60196 United States

Certification

Name: Jason T. Kunze

Date: March 12, 2010

Applicant's Tracking Number: 049423.001000

Correspondence: Yes

Registration #: TXU001641780

Service Request #: 1-356227849

Nixon Peabody LLP
Jason T. Kunze
300 South Riverside Plaza Suite 1600
Chicago, IL 60606-6613 United States

**EXHIBIT F
TO
THIRD AMENDED COMPLAINT**

Certificate of Registration



This Certificate issued under the seal of the Copyright Office in accordance with title 17, *United States Code*, attests that registration has been made for the work identified below. The information on this certificate has been made a part of the Copyright Office records.

A handwritten signature in black ink that reads "Marybeth Peters".

Register of Copyrights, United States of America

Registration Number
TXU 1-645-268

Effective date of registration:
March 25, 2010

Title

Title of Work: cncpbase.hh

Nature of Work: Literary Work

Completion/Publication

Year of Completion: 2001

Author

Author: Motorola Inc.

Author Created: text, editing, computer program

Work made for hire: Yes

Citizen of: United States

Domiciled in: United States

Year Born: 1928

Copyright claimant

Copyright Claimant: Motorola Inc.

1303 East Algonquin Road, Schaumburg, IL, 60196, United States

Rights and Permissions

Organization Name: Motorola Inc.

Telephone: 847-576-5000

Address: 1303 East Algonquin Road

Schaumburg, IL 60196 United States

Certification

Name: Jason T. Kunze

Date: March 23, 2010

Applicant's Tracking Number: 049423.001000

Registration #: TXU001645268

Service Request #: 1-366644778

Nixon Peabody
Jason T. Kunze
300 South Riverside Plaza Suite 1600
Chicago, IL 60606-6613 United States

EXHIBIT D

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

UNITED STATES OF AMERICA

v.

CONCORD MANAGEMENT &
CONSULTING LLC,

Defendant.

Criminal Action No. 18-cr-0032-2 (DLF)

ORDER

Before the Court is Defendant Concord Management and Consulting LLC’s Motion for Discovery Regarding Selective Prosecution, Dkt. 61. For the reasons stated during the hearing held on October 15, 2018, the Court denies Concord’s motion.

A criminal defendant must present “some evidence tending to show the existence of” (1) discriminatory effect and (2) discriminatory intent to prevail on a motion for discovery regarding a selective prosecution claim. *United States v. Armstrong*, 517 U.S. 456, 468–69 (1996). To show discriminatory effect, Concord must make a “credible showing of different treatment of similarly situated persons.” *Id.* at 470. And persons are similarly situated “when their circumstances present no distinguishable legitimate prosecutorial factors that might justify making different prosecutorial decisions with respect to them.” *Branch Ministries v. Rossotti*, 211 F.3d 137, 145 (D.C. Cir. 2000) (quoting *United States v. Hastings*, 126 F.3d 310, 315 (4th Cir. 1997)). To show discriminatory purpose, Concord must present credible evidence that the Special Counsel is prosecuting Concord “because of” its Russian nationality. *Wayte v. United States*, 470 U.S. 598, 610 (1985). Concord has not satisfied either requirement.

Concord relies on a host of media reports and a few miscellaneous court filings to show discriminatory effect. Media outlets reported that former Ukrainian government officials disseminated documents implicating Paul Manafort and posted social media messages criticizing then-candidate Donald Trump. Concord's Mot. at 8–9. Others reported a 2016 meeting between an envoy representing the Crown Princes of Saudi Arabia and Abu Dhabi, Donald Trump Jr., a Lebanese-American businessman, an Israeli social-media-manipulation specialist, and the founder of a private military contractor. *Id.* at 9–10. The discussions allegedly involved a proposed “online manipulation program designed to help elect then-candidate Trump by using thousands of fake accounts to promote him on Facebook.” *Id.* at 9–10. Other news reports stated that a former MI6 intelligence agent acted as an anonymous source for media reports about candidate Trump and that he, among other things, disseminated a dossier of opposition research about Trump. *Id.* at 10–11. And yet another report alleged that Iran used Facebook to spread disinformation worldwide. *Id.* at 6 n.2. Concord also relies on a 2016 Federal Election Commission complaint that alleges that two Chinese nationals funneled illegal campaign contributions through a U.S. corporation. *Id.* at 13. And it relies on another complaint and a Federal Election Commission Conciliation Agreement that allege that the Australian Labor Party sent Australian nationals as delegates to serve as volunteers with the Bernie 2016 campaign organization. *Id.* at 14, Exs. C, D.

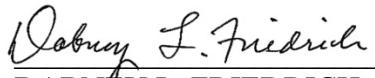
None of these allegations involves different treatment of “similarly situated persons.” *Armstrong*, 517 U.S. at 470. True, Concord’s examples involve foreign nationals and political candidates. But none of its examples is sufficiently similar to the conspiracy alleged here. Count one charges Concord, two other entities, and 13 individuals with conspiring to defraud the United States and interfere with the U.S. political system. It alleges that the co-conspirators,

among other things, created deceptive U.S. personas, social media pages, and social media groups to attract U.S. audiences and sow discord, used computer infrastructure to hide their Russian identities and affiliations, obtained visas under false pretenses, and destroyed emails to cover their tracks. *See* Indictment ¶¶ 2–85. And Concord has made no attempt to explain whether there are “legitimate prosecutorial factors,” including insufficient evidence, that could explain why the other foreign nationals it has identified have not been charged to date. *See Branch Ministries*, 211 F.3d at 14. Put simply, Concord has not made the “credible showing of different treatment of similarly situated persons” required to obtain discovery. *Armstrong*, 517 U.S. at 469.

To show discriminatory intent, Concord points to the Special Counsel’s appointment order. The order cites the Attorney General’s “responsibility . . . to ensure a full and thorough investigation of the Russian government’s efforts to interfere in the 2016 presidential election.” Concord’s Mot. Ex. A at 1 (Appointment Order), Dkt. 61-1. And it establishes the Special Counsel’s authority to “conduct the investigation confirmed by then-FBI Director James B. Comey in testimony before the House Permanent Select Committee on Intelligence on March 20, 2017,” which includes the investigation of “any links and/or coordination between the Russian government and individuals associated with the campaign of President Donald Trump.” *Id.*

But although the appointment order explicitly refers to the Russian government, it does not suggest that the Special Counsel is prosecuting Concord because Concord is Russian. To the extent the appointment order suggests any prosecutorial motive at all, it suggests that the Special Counsel is prosecuting individuals and entities because of their involvement in “the Russian government’s efforts to interfere in the 2016 presidential election,” *id.*—not because of their Russian nationality.

Concord has shown neither discriminatory effect nor discriminatory intent. Accordingly, its motion for discovery is **DENIED**.


Dabney L. Friedrich
DABNEY L. FRIEDRICH
United States District Judge

Date: October 16, 2018

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA,

NO. CR19-010RSM

Plaintiff,

V.

HUAWEI DEVICE CO., LTD.,
HUAWEI DEVICE USA, INC.,
Defendants.

**ORDER DENYING DEFENDANTS'
MOTION TO DISMISS FOR
SELECTIVE PROSECUTION, OR IN
THE ALTERNATIVE, FOR
DISCOVERY**

The Court, having considered the parties' briefing and the relevant record on the Defendants' Motion to Dismiss for Selective Prosecution, or in the Alternative, for Discovery, HEREBY DENIES the Motion.

DATED this day of August, 2019.

RICARDO S. MARTINEZ
Chief United States District Judge

1 Presented by:
2 TESSA M. GORMAN
3 First Assistant United States Attorney
4 (Acting Under Authority Conferred by 28 U.S.C. § 515)

5
6 s/Todd Greenberg
7 TODD GREENBERG
8 THOMAS WOODS
9 SIDDHARTH VELAMOOR
10 Assistant United States Attorneys
11 700 Stewart Street, Suite 5220
12 Seattle, WA 98101-1271
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28